SYMANITRON

Инновационные
промышленные сети

Руководство по настройке коммутаторов серии SEWM10A-D

Оглавление

Введение

Данный документ содержит информацию о настройках и возможностях программного обеспечения коммутаторов серии SEWM10A-D. Кроме того, в документе приводится детальная информация по настройке коммутаторов с помощью WEB-интерфейса.

Структура документа

Данное руководство включает следующую информацию:

Основная информация	Описание
1. Информация о продукте	• Описание продукта • Возможности программного обеспечения
2. Способы подключения к устройству	• Обзор возможностей • Подключение через консольный порт • Подключение с использованием Telnet • Подключение через Web-интерфейс
3. Управление	• Перезагрузка • Загрузка заводских настроек • Запись текущих настроек • Загрузка/Выгрузка файла конфигурации
4. Основные настройки	• Информация о системе • Настройки системы • Уровень загрузки CPU • Обновление прошивки (HTTP, SFTP)
5. Настройки IP	• Настройка IP адресов • Настройка ARP • Настройка DHCP
6. Часы	• Настройка часов • SNTP
7. Настройка портов	• Настройка статуса портов • Статистика портов
8. Настройка QoS	• Сопоставление приоритетов очередей на основе портов • 802.1Q Сопоставление приоритетов очереди на основе заголовков • IEEE802.1p • Сопоставление приоритетов очередей на основе DSCP • QCL • Фиксация скорости доступа на основе портов • Фиксация скорости доступа на основе очередей • Планирование очереди на основе порта • Формирование трафика на основе портов • Подавление широковещательных штормов

9. Безопасность	• Управление пользователями • Настройки аутентификации при подключении к устройству • Настройки SSH • Настройки SSL • Управление доступом • SNMP v1/v2c/v3 • Настройки RMON • Настройки TACACS+ • Настройки RADIUS
10. Сеть	• Безопасность портов • Настройки IEEE802.1X • Настройка ACL
11. Агрегирование портов	• Статистика • Настройка LACP
12. Обнаружение петель (Loop)	• Настройка функционала обнаружения петель
13. Мультикастовые протоколы	• IGMP Snooping • GMRP
14. Протокол LLDP	• Настройка функций протокола
15. MAC-адреса	• Настройка MAC-адресов
16. VLAN	• Настройка VLAN • Настройка PVLAN • GVRP
17. Резервирование	• Sy2-Ring • Sy2-RP • STP/RSTP/MSTP
18. Аварийные сообщения	• По питанию • О проблемах с памятью или CPU • По портам • По кольцевому резервированию • По конфликтам IP или MAC адресов • О потере пакетов и CRC
19. Зеркалирование портов	• Настройка функционала зеркалирования портов
20. Системный журнал	• Ведение системного журнала Syslog

Условные обозначения

1. Условные обозначения в тексте

Формат	Описание
< >	Скобки < > обозначают «кнопки». Например, нажмите кнопку <Apply>
[ ]	Скобки [ ] обозначают имя окна или имя меню. Например, нажмите пункт меню [File]
{ }	Скобки { } обозначают группу. Например {IP address, MAC address} означает, что IP адрес и MAC адрес составляют группу и могут быть настроены и показаны вместе.
→	Мультиуровневое меню разделяется посредством знака «→». Например, Start→AllPrograms→Accessories. Нажмите меню [Start], войдите в подменю [All programs], затем войдите в подменю [Accessories].
/	Выбор одной, двух или более опций при помощи символа «/». Например, «Add/Subtract» означает добавить или удалить.
~	Знак «~» обозначает диапазон значений. Например, «1~255» указывает на диапазон от 1 до 255

2. Условные обозначения CLI

Формат	Описание
Bold	Означает Команды и ключевые слова. Например, **show version** будет показываться с использованием шрифта **Bold**
Italic	Параметры, для которых вы указываете значения с помощью шрифта *italic.* Например, для команды **show vlan** *vlan id* указывается актуальное значение команды *vlan id* посредством шрифта *italic*

3. Условные символы

Символ	Описание
 **Предостережение**	Эти вопросы требуют внимания во время работы с устройством при настройке, а также дают дополнительную информацию.
 **Заметка**	Необходимые пояснения к содержимому выполняемых операций с устройством.
 **Внимание**	Вопросы, требующие особого внимания. Некорректная работа с устройством может привести к потере данных или повреждению.

1. Информация об устройстве

1.1. Основная информация о коммутаторе

Промышленные коммутаторы серии SEWM10A-D могут использоваться в различных областях промышленности: системах передачи данных в энергетике, на транспорте, в горнодобывающей промышленности и т.д. Данные серии коммутаторов поддерживает протокол MSTP и проприетарный протокол Sy2-Ring, гарантируя надежную работу системы. Серия коммутаторов SEWM10A-D поддерживает функцию цифровой диагностики оптических модулей SFP, которая обеспечивает контроль мощности передачи и приема птического приемопередатчика в режиме реального времени.

1.2. Функциональные возможности ПО

Программное обеспечение коммутатор SEWM10A-D поддерживает множество различных функций:

- Протоколы кольцевого резервирования: RSTP/STP, Sy2-Ring и MSTP;
- Протоколы мультиадресной рассылки (Multicast): IMGP Snooping, GMRP, Static;
- Функции коммутации: VLAN, PVLAN, GVRP, QoS, ARP;
- Управление пропускной способностью: статическая агрегация портов, LACP, ограничение скорости порта и подавление широковещательных штормов;
- Безопасность: управление пользователями, управление доступом, SSH, SSL, TACACS+, RADIUS, IEEE802.1X и ACL;
- Протоколы синхронизации времени: SNMP, PTP;
- Управление устройством: обновление программного обеспечения, загрузка/выгрузка файла конфигурации, запись и выгрузка журнала;
- Диагностика устройства: зеркалирование портов (port mirroring), LLDP, проверка статуса соединения (Link check) и защита от петель (Loop Detection);
- Система тревожных оповещений: ошибка порта (port alarm), ошибка питания (power alarm), ошибка кольца (ring alarm), оповещения о конфликтах IP и MAC адресов, ошибки использования памяти и CPU;
- Сетевой доступ к устройству и управление: CLI, Telnet, Web, NMS Symanitron, SNMP;

2. Подключение к устройству

Устройство можно настраивать одним из четырех нижеперечисленных способов:

- через консольный порт
- посредством Telnet
- с использованием WEB-интерфейса
- с помощью программы Symanitron NMS

2.1. Варианты просмотра и отображения

Когда пользователь (администратор сети) подключается к устройству посредством CLI через консольный порт или Telnet, он имеет возможность, используя различные команды, получать информацию о состоянии устройства и выполнять настройки коммутатора:

Табл. 1

Подсказка	Тип отображения	Функция	Команда
SWITCH #	Привилегированный режим	Загрузить/выгрузить конфигурационный файл Вернуться к заводским настройкам Отобразить результаты команды ping Перезагрузить коммутатор Записать текущую конфигурацию Обновить ПО	Введите «**Configure terminal**» для переключения из привилегированного режима в режим настройки Введите «**exit**» для возврата в основной режим
SWITCH (config) #	Режим Настройки	Настроить все функциональные возможности коммутатора	Введите «**exit**» или «**end**» для возврата в привилегированный режим

Когда выполняется настройка коммутатора посредством сервиса CLI, символ «?» может использоваться для получения помощи по используемым командам. Для получения помощи, нужно ввести описание параметров, например, <1,255> означает диапазон чисел, <H.H.H.H> означает IP адрес, <xx:xx:xx:xx:xx:xx> означает MAC адрес, <word31> означает диапазон строк 1~31. Также символы ↑ и ↓ могут использоваться для просмотра недавно использованных команд.

2.2. Подключение через консольный порт

Пользователь может подключиться к устройству посредством консольного порта с помощью HyperTerminal операционной системы Windows или с помощью другого программного обеспечения, которое поддерживает подключение по последовательному порту, например HTT3.3. В примере ниже показано, как использовать консольный порт и HyperTerminal для доступа к коммутатору.

1. Подключите USB кабель к ПК и консольному интерфейсу устройства (кабель должен быть оснащён разъёмом USB с одной стороны и Mini USB с другой).
2. Запустите HyperTerminal в основном окне Windows, нажмите [Start]—>[All Programs]—>[Accessories]—>[Communications]—>[Hyper Terminal] (см. Рис. 1).

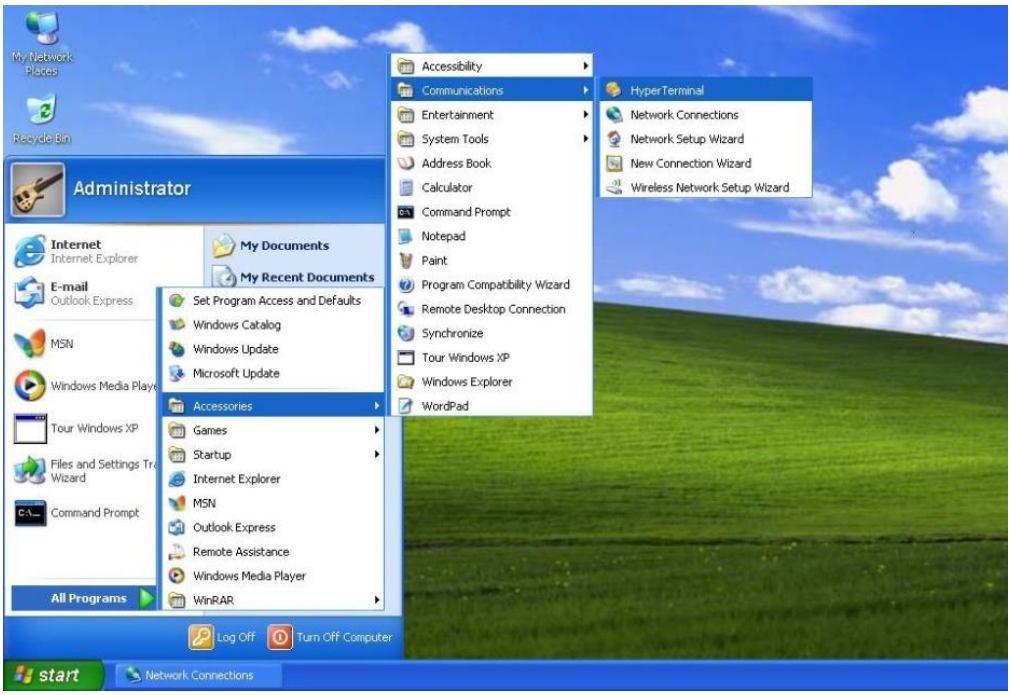


Рис. 1. Запуск HyperTerminal

3. Создайте новое подключение, например, с именем «Switch» (см. рис. 2).

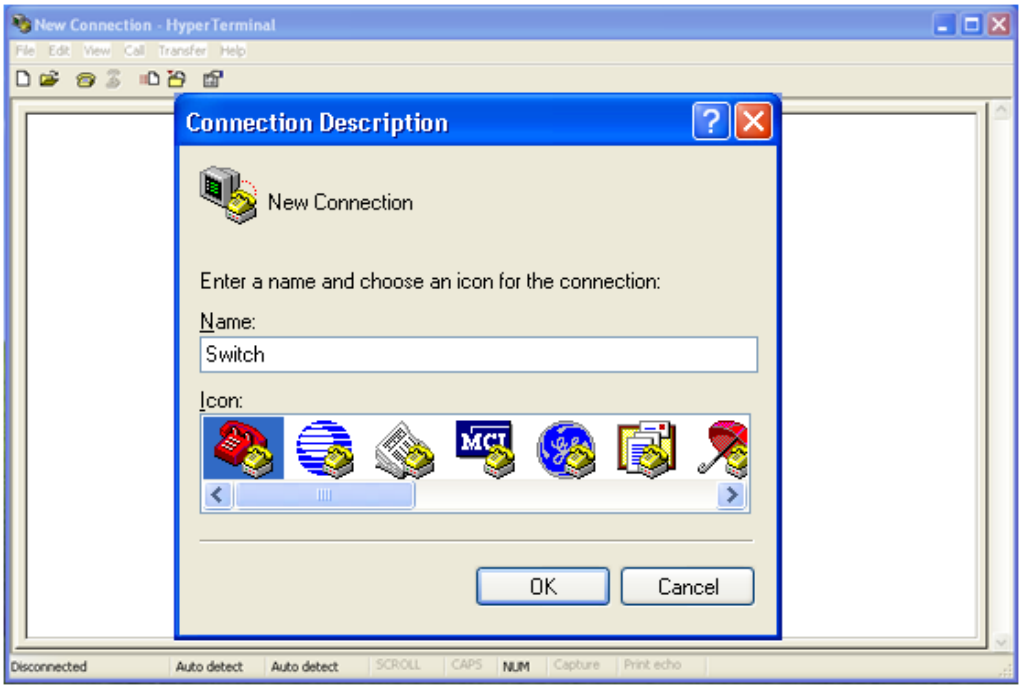


Рис. 2. Создание нового подключения

4. Выберите COM порт для подключения.

Рис. 3. Выбор COM порта для подключения

Для подтверждения COM порта нажмите [My Computer]->[Property]->[Hardware]->[Device Manager]->[Port] и проверьте работу порта, который используется как консольный.

5. Настройте параметры COM порта. Скорость (Baud rate): 115200, Биты данных (Data bits): 8, Чётность (Parity): None, Стоповые биты (Stop bits): 1, Контроль потока (Flow control): None.

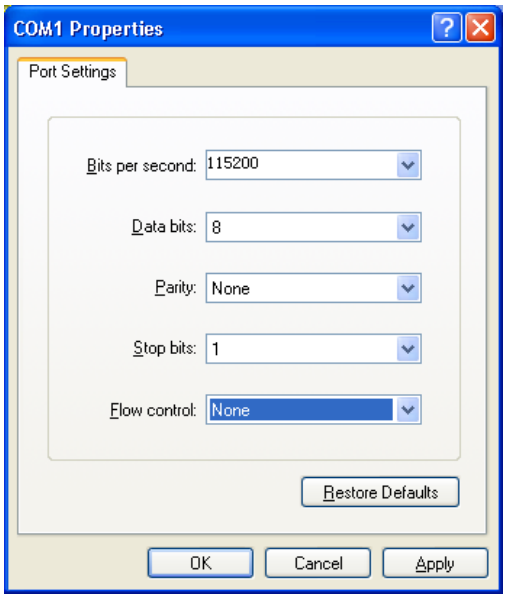


Рис. 4. Настройка параметров COM порта

6. Нажмите <OK> для входа в командную строку CLI. Нажмите <Enter> для входа в пользовательский режим. Введите имя пользователя по умолчанию «admin» и пароль «123», чтобы войти в привилегированный режим. В дальнейшем Вы также можете ввести имя пользователя и пароль, созданные самостоятельно.

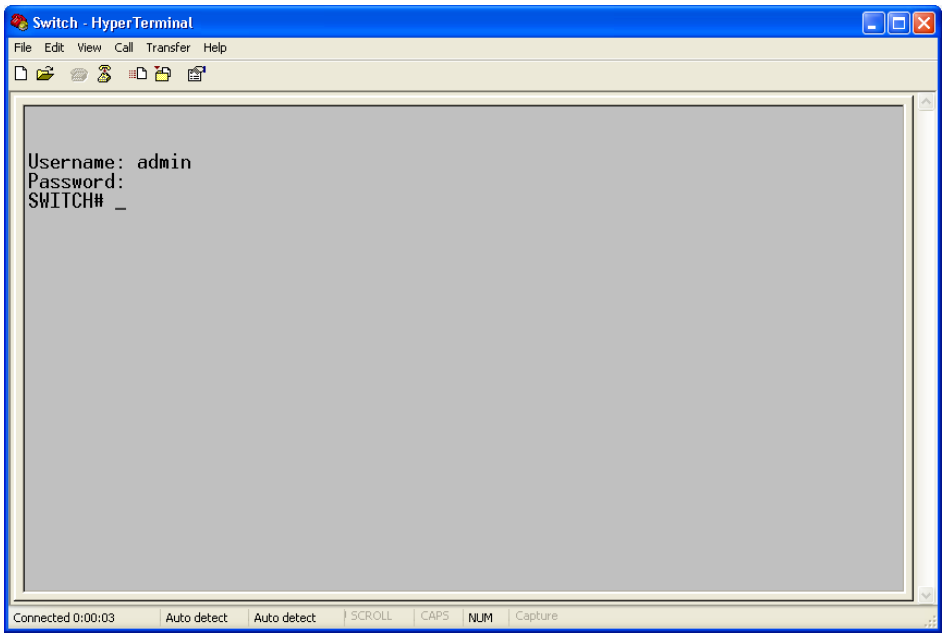


Рис. 5. Экран CLI

2.3. Подключение к коммутатору посредством Telnet

1. Подключите любой RJ45 порт коммутатора к Ethernet порту ПК.
2. Откройте <Выполнить> на ПК, там введите «telnet IP-адрес», по умолчанию IP-адрес - 192.168.0.2.

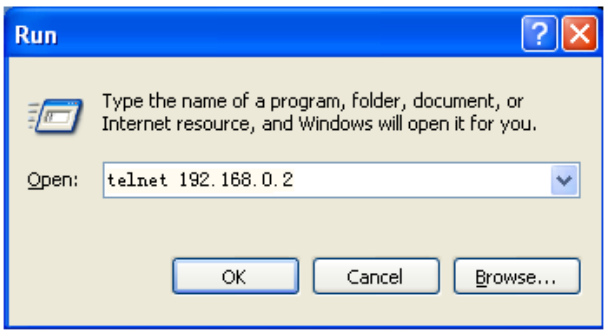


Рис. 6. Доступ через Telnet

При подтверждении IP-адреса, пожалуйста, обратитесь к разделу «IP адрес» настоящего руководства для получении информации о IP адресе.

3. В интерфейсе Telnet введите имя пользователя «admin» и пароль «123» для входа в коммутатор. В дальнейшем Вы также можете ввести имя пользователя и пароль, созданные самостоятельно.

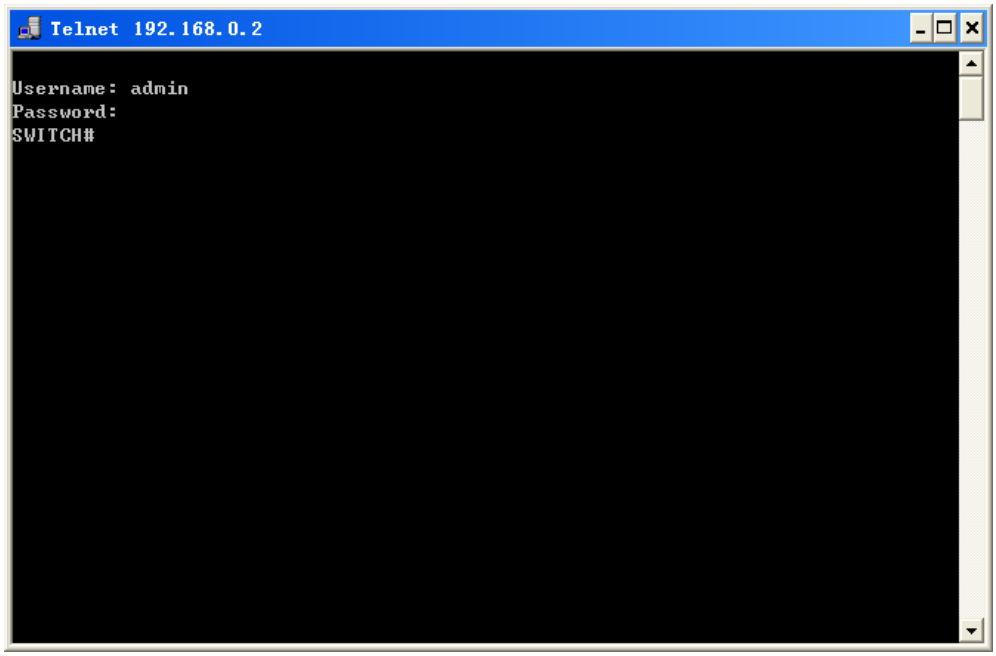


Рис. 7. Интерфейс терминала Telnet

2.4. Доступ через WEB-интерфейс

1. Подключите любой RJ45 порт коммутатора к Ethernet порту ПК.
2. Введите IP адрес коммутатора в web-браузере (IP адрес по умолчанию - 192.168.0.2). Появится диалоговое окно авторизации, показанное ниже. Введите:

   Логин - **admin**

   Пароль – **123**

   Нажмите кнопку <Login>.

При использовании Internet Explorer, рекомендуется использовать версию не ниже 8.0.

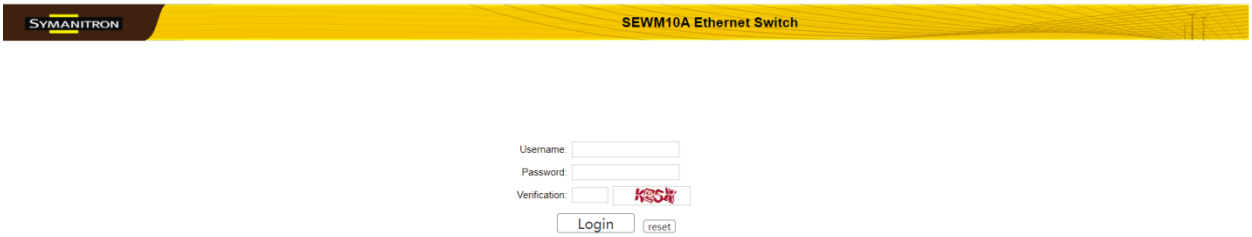


Рис. 8. Авторизация через WEB-интерфейс

3. После подключения к Web-интерфейсу коммутатора вы увидите «навигационное дерево» (меню) в левой части экрана:

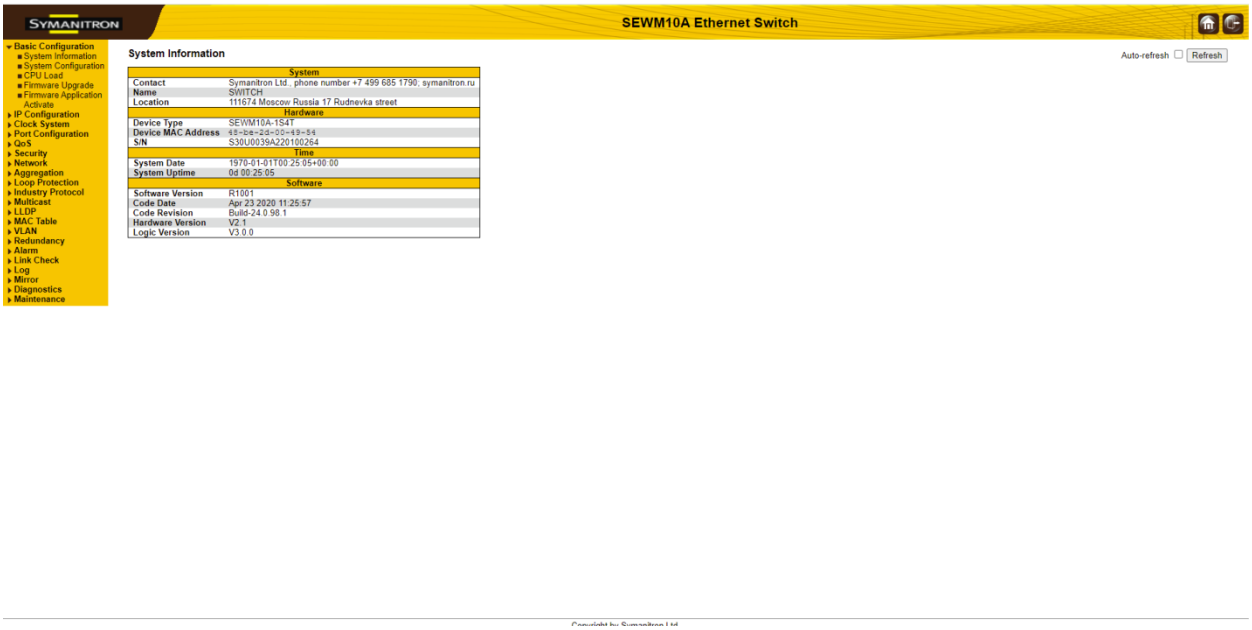


Рис. 9. Страница WEB-интерфейса

У вас есть возможность сворачивать или разворачивать меню навигации. Нажмите кнопку  для перехода к основному меню или кнопку  для выхода из WEB-интерфейса.

Как показано на рисунке 10, страница конфигурации/просмотра каждого модуля настройки содержит несколько кнопок управления. Например, вы можете нажать <Submit>, чтобы текущая конфигурация была активирована. Нажмите <Reset>, чтобы

отменить текущую конфигурацию и использовать конфигурацию, которая была активирована. Нажмите <Cancel>, чтобы закрыть страницу конфигурации и вернуться к предыдущей странице настроек. Нажмите <Refresh>, чтобы обновить информацию на текущей странице. Вы также можете выбрать «Автообновление», чтобы информация обновлялась автоматически с интервалом в 4 секунды или нажмите <Clear>, чтобы очистить и перезапустить статистику.

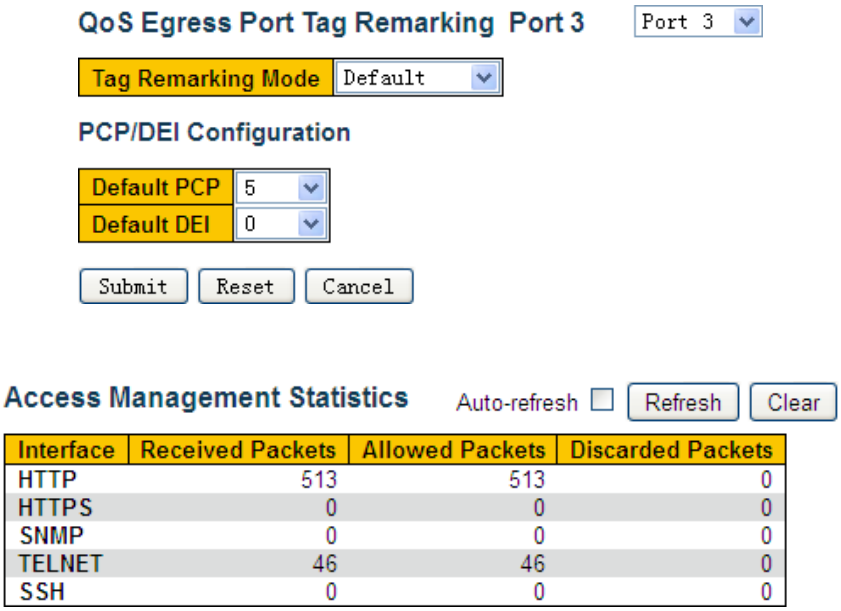


Рис. 10. Интерфейс статистики и конфигурации

3. Управление устройством

1. Перезагрузка устройства.

Рис. 11. Перезагрузка устройства

Перед перезагрузкой устройства необходимо подтвердить, нужно ли сохранять текущую конфигурацию. Если вы выберете «Yes», после перезагрузки коммутатор запустит текущую конфигурацию. Если вы выберете «No», коммутатор запустит предыдущую сохраненную конфигурацию. Если конфигурация не была сохранена, после перезагрузки коммутатор восстановит конфигурацию по умолчанию.

2. Восстановление заводских настроек.

Рис. 12. Восстановление заводских настроек

После того как вы изменили заводские установки и записали новые параметры, необходимо перезагрузить устройство для того, чтобы новые параметры вступили в силу.

3. Сохранение текущей рабочей конфигурации.

Рис. 13. Сохранение текущих настроек

4. Выгрузка файла из коммутатора на локальный сервер.

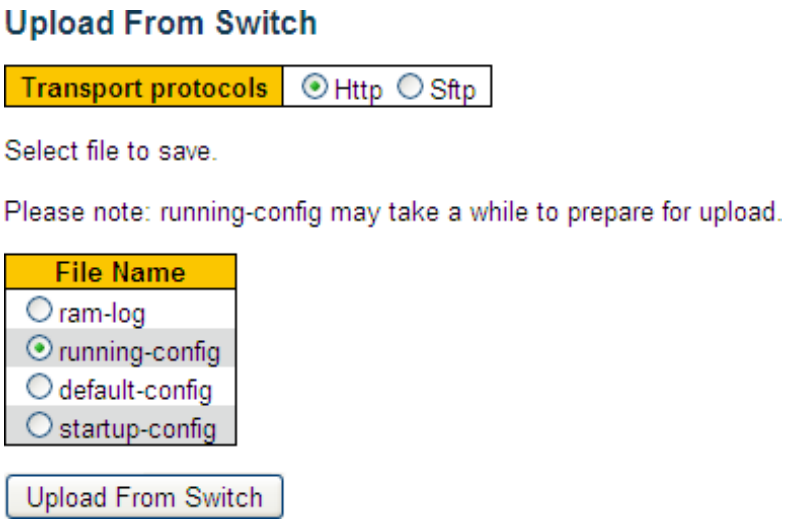


Рис. 14. Выгрузка файла с использованием HTTP

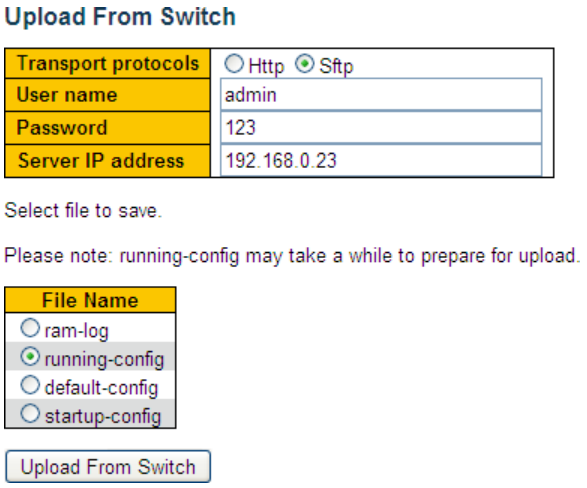


Рис. 15. Выгрузка файла с использованием SFTP

Имя пользователя, пароль ({User name, Password})
Диапазон значений: {1~63 символов, 1~63 символов}
Описание: ввод имени пользователя и пароля, созданного на сервере SFTP.
IP-адрес сервера (Server IP address)
Формат: A.B.C.D
Описание: Настройка IP-адреса сервера SFTP.

- Для передачи файлов посредством SFTP необходимо настроить имя пользователя SFTP, пароль и IP-адрес сервера SFTP.
- В процессе передачи файлов нужно следить за тем, чтобы сервер SFTP находился в рабочем состоянии.

В файле «ram-log» записывается информация журнала, «running-config» - это текущий рабочий файл конфигурации коммутатора, «default-config» - это файл конфигурации по умолчанию, а «startup-config» - это файл запуска коммутатора. Выберите файл и нажмите <Upload From Switch>, чтобы сохранить файл на локальном сервере.

5. Загрузка файла конфигурации с локального сервера в коммутатор.

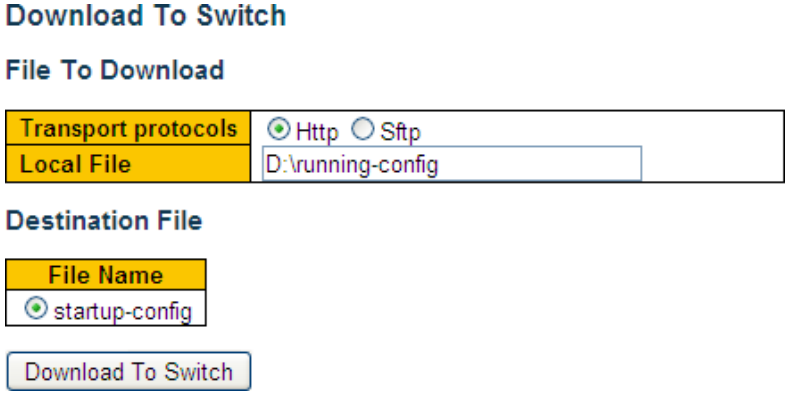


Рис. 16. Загрузка файла с использованием HTTP

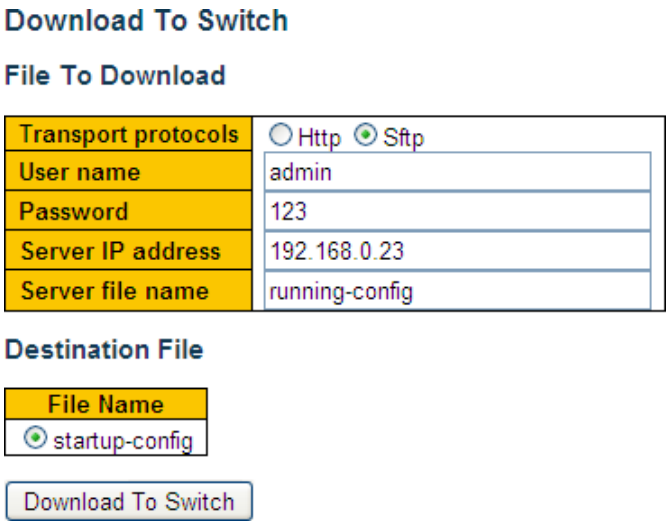


Рис. 17. Загрузка файла с использованием SFTP

Локальный файл (Local File)
Описание: выбор файла конфигурации, сохраненного на локальном сервере.
Имя пользователя, пароль ({User name, Password})
Диапазон значений: {1~63 символов, 1~63 символов}
Описание: ввод имени пользователя и пароля, созданного на сервере SFTP.
IP-адрес сервера (Server IP address)
Формат: A.B.C.D
Описание: Настройка IP-адреса сервера SFTP.
Имя файла на сервере (Server file name)
Диапазон значений: 1~63 символов
Описание: выбор файла, записанного на локальном сервере.

- Для передачи файлов посредством SFTP необходимо настроить имя пользователя SFTP, пароль и IP-адрес сервера SFTP.
- В процессе передачи файлов нужно следить за тем, чтобы сервер SFTP находился в рабочем состоянии.

Вы можете загрузить конфигурационный файл с локального сервера в коммутатор как новый загрузочный файл. Новый загрузочный файл заменит оригинальный файл «startup-config». Нажмите <Download To Switch> для загрузки конфигурационного файла из локального сервера.

6. Настройка через порт USB
Выгрузка/Загрузка файлов конфигурации с помощью внешнего флэш-накопителя.

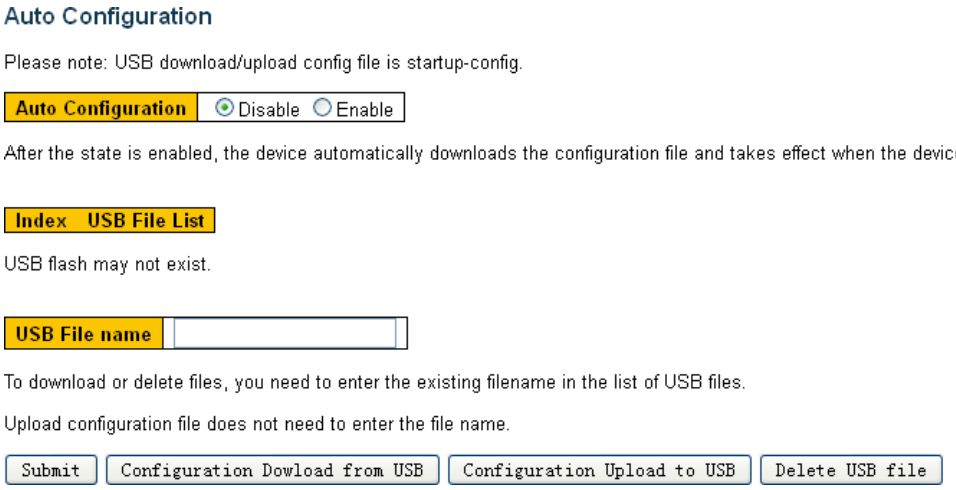


Рис. 18. Выгрузка/Загрузка файлов с использованием USB

4. Основные настройки

4.1. Основная информация о коммутаторе

Основная информация о коммутаторе включает имя устройства, тип устройства, MAC-адрес, серийный номер, системные дату и время, версию прошивки.

System Information

System	
Contact	Symanitron Ltd., phone number +7 499 685 1790; symanitron.ru
Name	SWITCH
Location	111674 Moscow Russia 17 Rudnevka street
Hardware	
Device Type	SEWM10A-1S4T
Device MAC Address	48-be-2d-00-49-54
S/N	S30U0039A220100264
Time	
System Date	1970-01-01T00:28:50+00:00
System Uptime	0d 00:28:50
Software	
Software Version	R1001
Code Date	Apr 23 2020 11:25:57
Code Revision	Build-24.0.98.1
Hardware Version	V2.1
Logic Version	V3.0.0

Рис. 19. Основная информация о коммутаторе

4.2. Настройки системы

Настройки системы включают в себя контактную информацию, имя системы и местоположение.

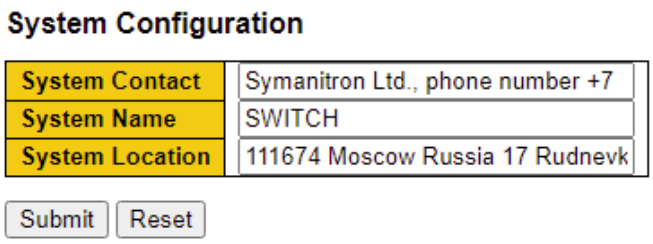


Рис. 20. Настройки системы

Контакты (System Contact)
Диапазон значений: 0~255 символов (символы ASCII от 32 до 126).
Имя системы (System Name)
Диапазон значений: 0~255 символов (буквы A~Z/a~z, цифры 0~9, знак минуса -. Первый символ должен быть буквой, при этом первый или последний символ не должны быть знаком минуса).
Местоположение (System Location)
Диапазон значений: 0~255 символов (символы ASCII от 32 до 126).

4.3. Загрузка CPU

Нагрузка измеряется как среднее значение за последние 100 мс, 1 с и 10 секунд, как показано на рисунке 21.

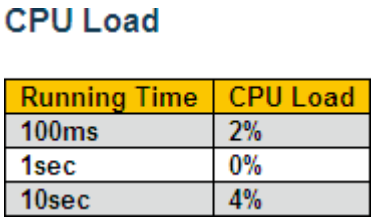


Рис. 21. Загрузка CPU

4.4. Обновление прошивки

Обновление прошивки может помочь коммутатору улучшить его работу. Для коммутаторов этой серии обновление прошивки включает обновление версии загрузчика (Boot) и обновление версии системного программного обеспечения. Версия загрузчика должна быть обновлена до версии системного программного обеспечения. Если версия загрузчика не меняется, вы можете обновить только версию системного программного обеспечения. Для обновления прошивки требуется поддержка HTTP / SFTP.

4.4.1. Обновление прошивки через HTTP

1. Обновление прошивки.

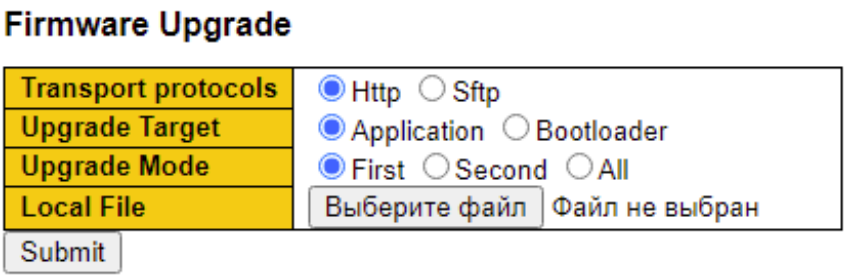


Рис. 22. Обновление прошивки через HTTP

Цель обновления (Upgrade Target)
Опции: ПО/Загрузчик (Application/Bootloader).
Функция: Выбор цели обновления.
Режим обновления (Upgrade Mode)
Опции: Первый/Второй/Все (First/Second/All)
Описание: в коммутатор можно загрузить две версии программного обеспечения, которые могут быть одинаковыми или разными. «All» загружает версию 1 и версию 2.
Локальный файл (Local File)
Функция: выбор файла обновления, хранящегося на локальном сервере.

2. Когда обновление будет завершено, пожалуйста, активируйте версию программного обеспечения и перезагрузите устройство. Откройте страницу «System Information», чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

Рис. 23. Обновление завершено

- После завершения обновления нужно активировать новую версию ПО. Для этого перезагрузите коммутатор.
- В случае сбоя обновления не перезагружайте устройство, чтобы избежать потери файла с ПО.

4.4.2. Обновление прошивки через SFTP

Протокол безопасной передачи файлов (SFTP) - это протокол передачи файлов на основе SSH. Он обеспечивает зашифрованную передачу файлов для обеспечения безопасности.
В следующем примере используется MSFTP для описания конфигурации сервера SFTP и процесса обновления прошивки.

1. Добавление пользователя SFTP. Введите пользователя и пароль, например admin и 123. Установите номер порта на 22. Введите путь для сохранения файла версии микропрограммы в поле Root path.

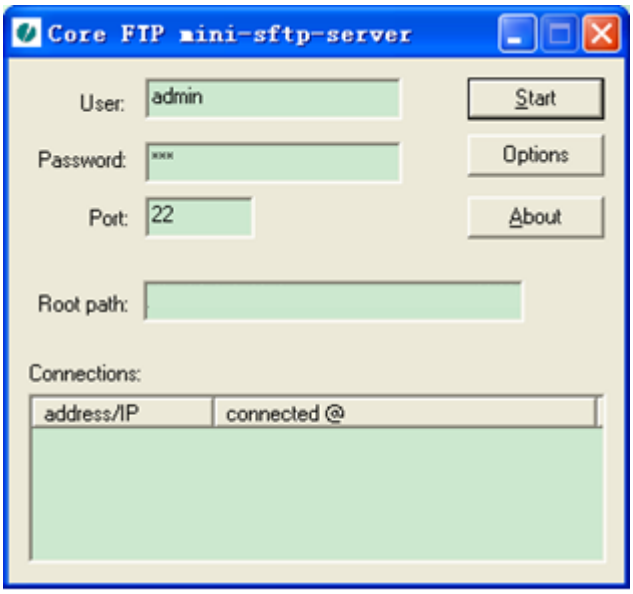


Рис. 24. Добавление пользователя SFTP

2. Обновление прошивки

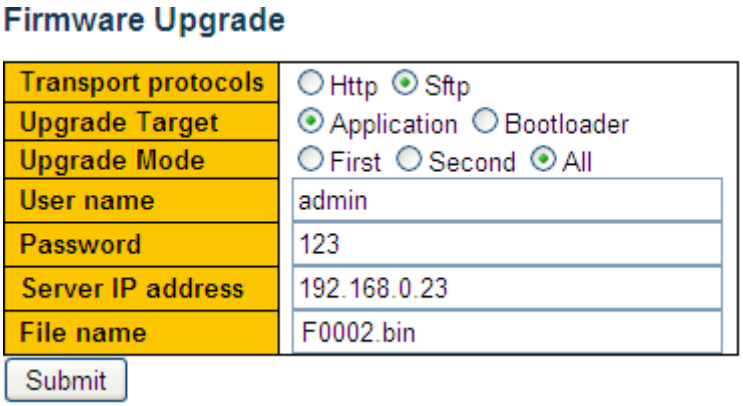


Рис. 25. Добавление прошивки через SFTP

Цель обновления (Upgrade Target)
Опции: ПО/Загрузчик (Application/Bootloader).
Функция: выбор цели обновления.
Режим обновления (Upgrade Mode)
Опции: Первый/Второй/Все (First/Second/All)

Описание: в коммутатор можно загрузить две версии программного обеспечения, которые могут быть одинаковыми или разными. «All» загружает версию 1 и версию 2.

Имя пользователя, пароль ({User name, Password})

Диапазон значений: {1~63 символов, 1~63 символов}

Описание: ввод имени пользователя и пароля, созданного на сервере SFTP.

IP-адрес сервера (Server IP address)

Формат: A.B.C.D

Описание: настройка IP-адреса сервера SFTP.

Имя файла (Server File name)

Диапазон значений: 1~63 символов

Описание: выбор файла прошивки, записанного на локальном сервере.

3. Когда обновление будет завершено, пожалуйста, активируйте версию программного обеспечения и перезагрузите устройство. Откройте страницу «System Information», чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

Рис. 26. Обновление завершено

- В процессе обновления прошивки не отключайте сервер SFTP.
- После завершения обновления перезагрузите устройство, чтобы активировать новую версию.
- В случае сбоя обновления не перезагружайте устройство, чтобы избежать потери файла ПО.

4.5. Активация версии приложения прошивки

1. Активация соответствующей версии приложения прошивки.

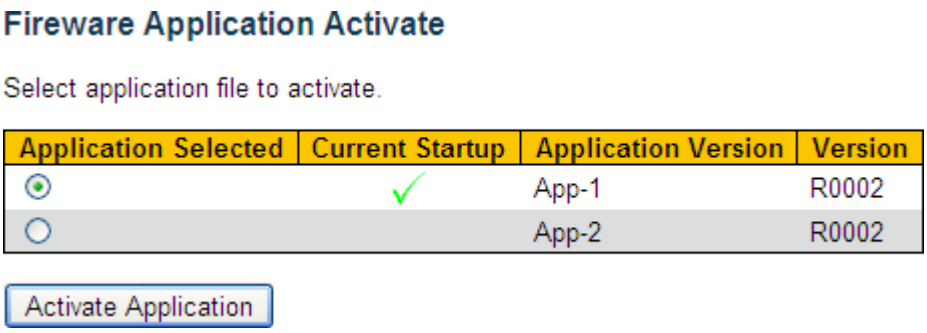


Рис. 27. Активация версии приложения прошивки

Выберите одну из версий и нажмите кнопку <Activate Application>, настроив версию, которая будет активной, то есть следующей загрузочной версией. Одновременно может быть активна только одна версия.

5. Настройки IP

5.1. Настройка IP-адреса

1. Отображение IP-адреса, используя консольный порт.

Подключитесь к коммутатору через консольный порт. Введите команду «show interface vlan 1» в привилегированном режиме режиме для проверки IP адреса коммутатора:

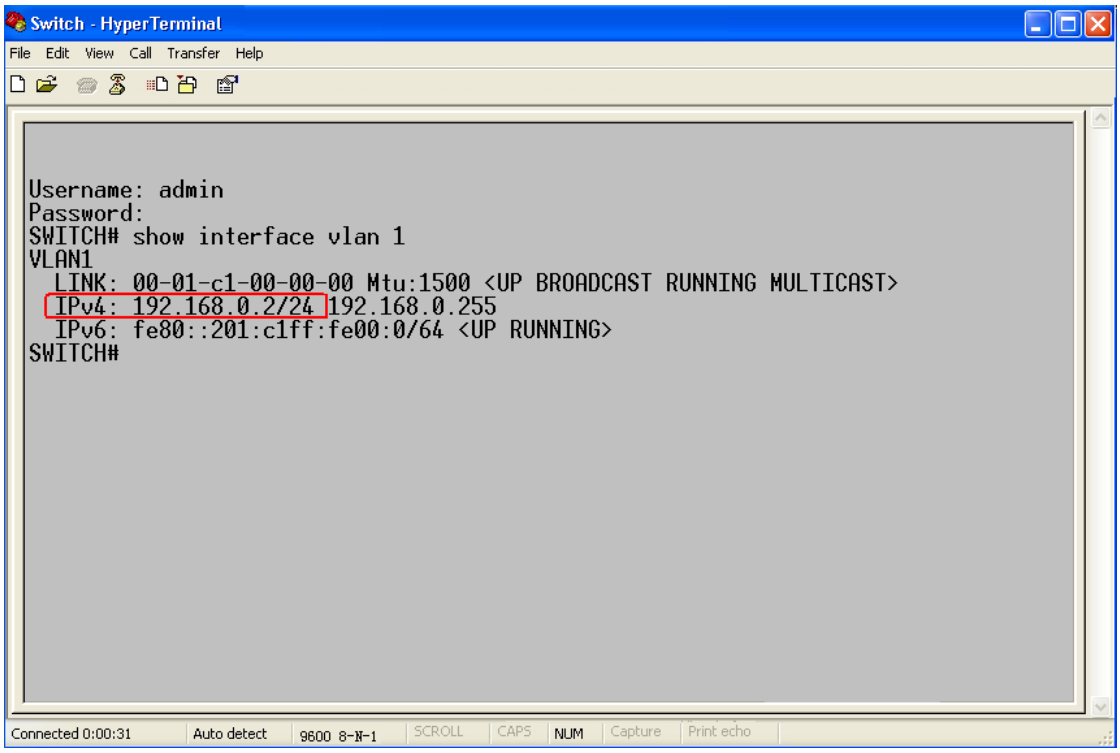


Рис. 28. Отображение IP адреса

2. Создание интерфейса IP.

Хосты в разных VLAN не могут связываться друг с другом. Их коммуникационные пакеты должны пересылаться маршрутизатором или коммутатором уровня 3 через IP-интерфейс. Коммутаторы этой серии поддерживают IP-интерфейсы, которые представляют собой виртуальные интерфейсы уровня 3, используемые для связи между VLAN. Вы можете создать один IP-интерфейс для каждой VLAN. Интерфейс используется для пересылки пакетов уровня 3 в VLAN.

3. Настройка IP-адреса

IP-адрес коммутатора можно настроить вручную или получить автоматически.

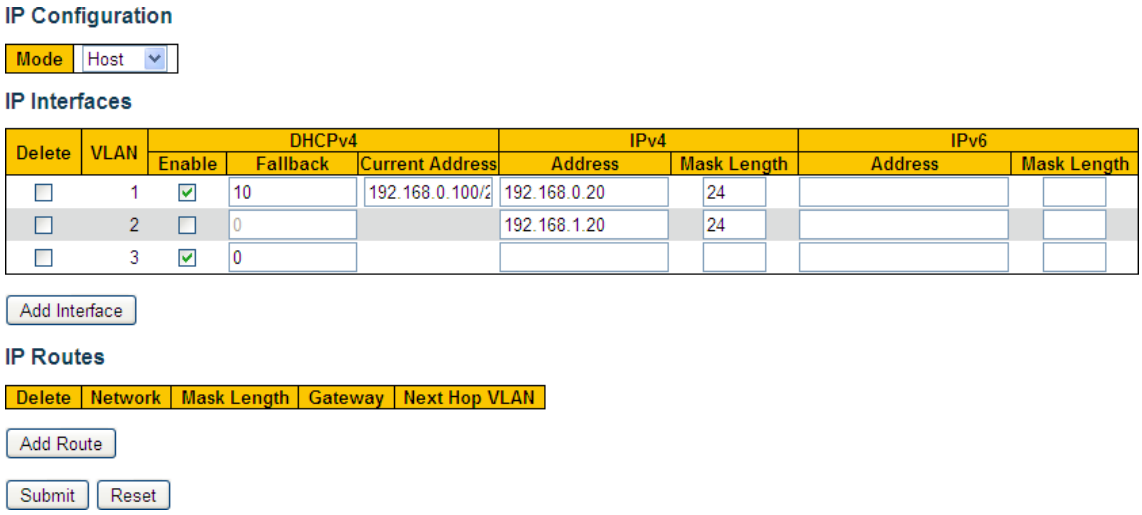


Рис.29. Настройка IP адреса

VLAN

Функция: настройка атрибута VLAN IP-интерфейса; порты в этой VLAN смогут получить доступ к IP-интерфейсу.

Включение DHCPv4 (DHCPv4-Enable)

Опции: Включить/Выключить (Enable/Disable)

Функция: отключение DHCPv4, настройка IP-адреса и маски вручную; включение DHCPv4, при этом коммутатор (как DHCP-клиент) автоматически получает IP-адрес через DHCP. В сети должен быть DHCP-сервер для назначения IP-адресов и масок клиентам.

Отсроченный DHCPv4 (DHCPv4-Fallback)

Диапазон значений: 0~4294967295 сек.

Функция: если значение не равно нулю, коммутатор получает определенное время для получения IP-адреса по протоколу DHCP. Если по истечении времени попытки закончатся неудачно, IP-адрес необходимо настроить вручную. Если значение равно 0, коммутатор неоднократно пытается получить IP-адрес, пока не получит его через DHCP. В этом случае нет необходимости настраивать IP-адрес вручную.

Текущий адрес DHCPv4 (DHCPv4-Current Address)

Функция: отображение IP-адреса и длины маски, автоматически получаемых от сервера DHCP. Если коммутатору не удается получить IP-адрес через DHCP, в поле «Current Address» отображаются IP-адрес и длина маски, настроенные вручную.

IP-адрес IPv4 (IPv4-Address)

Формат: A.B.C.D

Функция: Настройка IP-адреса вручную.

Длина маски IPv4 (IPv4-Mask Length)

Функция: маска подсети - это число длиной 32 бита, состоящее из строки «1» и строки «0». «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Длина маски - это число «1» в маске подсети.

Нажмите <Add Interface>, чтобы добавить новый IP-интерфейс; поддерживается максимум 8 интерфейсов.

- Каждый IP-интерфейс поддерживает один IP-адрес.
- IP-адреса разных сегментов сети должны быть настроены для разных IP-интерфейсов.

4. Просмотр IP-интерфейсов

IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
OS:lo	IPv6	fe80::1/64	
VLAN1	LINK	00-01-c1-00-00-00	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.100/24	
VLAN1	IPv6	fe80::201:c1ff:fe00:0/64	
VLAN2	LINK	00-01-c1-00-00-00	<BROADCAST MULTICAST>
VLAN2	IPv4	192.168.1.20/24	
VLAN2	IPv6	fe80::201:c1ff:fe00:0/64	
VLAN3	LINK	00-01-c1-00-00-00	<BROADCAST RUNNING MULTICAST>
VLAN3	IPv6	fe80::201:c1ff:fe00:0/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour Cache

IP Address	Link Address
192.168.0.184	VLAN1:44-37-e6-88-6e-90
fe80::201:c1ff:fe00:0	VLAN1:00-01-c1-00-00-00
fe80::201:c1ff:fe00:0	VLAN2:00-01-c1-00-00-00
fe80::201:c1ff:fe00:0	VLAN3:00-01-c1-00-00-00

Рис.30. Просмотр IP-интерфейсов

5.2. Протокол ARP

5.2.1. Введение

Протокол ARP разрешает сопоставление между IP-адресами и MAC-адресами посредством механизма запроса и ответа адресов. Коммутатор получает информацию о соответствии между IP-адресами и MAC-адресами других хостов в том же сегменте сети. Данный механизм также поддерживает статические записи ARP для указания сопоставления между IP-адресами и MAC-адресами. Динамические записи ARP периодически устаревают, обеспечивая согласование между записями ARP и фактическими приложениями.
Коммутаторы данной серии обеспечивают не только функцию коммутации уровня 2, но также функцию ARP для разрешения IP-адресов других хостов в том же сегменте сети, обеспечивая связь между NMS и управляемыми хостами.

5.2.2. Настройка через WEB-интерфейс

1. Настройка времени старения ARP.

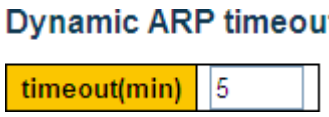


Рис.31. Настройка времени старения

Таймаут (timeout)
Диапазон значений: 0~60 мин.
Значение по умолчанию: 5 мин.
Функция: настройка времени устаревания ARP; если для времени устаревания установлено значение 0, устаревание запрещено.
Описание: время устаревания ARP - это продолжительность с момента добавления динамической записи ARP в таблицу до момента удаления записи из таблицы.

2. Добавление статической записи ARP.

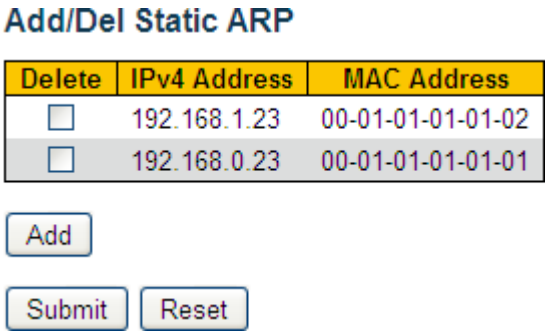


Рис.32. Добавление статической записи ARP

ARP
Настройка значений: {IP address, MAC address}
Формат: {A.B.C.D, HHHHHHHHHHHH} (H - шестнадцатеричное число)
Функция: настройка статической записи ARP.

Как правило, коммутатор автоматически изучает записи ARP. Ручная настройка не требуется.

Нажмите <Add>, чтобы добавить новую статическую запись ARP; поддерживается максимум 128 статических записей ARP.

5.3. Настройка DHCP

С постоянным расширением масштабов сетей и ростом их сложности, а также в условиях частого перемещения компьютеров (таких, например, как ноутбук) и их количества, превышающих количество выделяемых IP-адресов, протокол BootP, специально предназначенный для конфигурации статического хоста, постоянно теряет способность

удовлетворять реальные потребности в IP-адресах. Для быстрого доступа к сети, а также повышения коэффициента использования ресурсов IP-адресов действительно было необходимо разработать автоматический механизм для назначения IP-адресов на основе BootP. Для решения этих проблем был создан протокол DHCP (Dynamic Host Configuration Protocol, Протокол динамической настройки хостов).
Протокол DHCP использует модель взаимодействия клиент-сервер. Клиент отправляет запрос о конфигурации серверу, а сервер отвечает на параметры конфигурации, обеспечивая динамическую конфигурацию IP-адресов. Схема типичного варианта использования протокола DHCP показана на рисунке ниже.

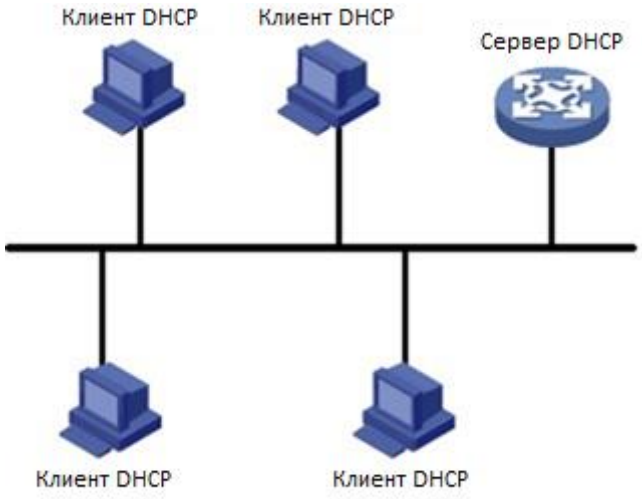


Рис. 33. Типичная схема DHCP

В процессе динамического получения IP-адресов сообщения рассылаются путем широковещательной рассылки, поэтому требуется, чтобы DHCP-клиент и DHCP-сервер находились в одном сегменте. Если они находятся в разных сегментах, клиент может связаться с сервером через DHCP Relay, чтобы получить IP-адреса и параметры конфигурации.

Протокол DHCP поддерживает два механизма распределения IP-адресов.
Статическое распределение: сетевой администратор статично привязывает фиксированные IP-адреса к нескольким конкретным клиентам, таким как, например, WWW-сервер, и отсылает привязанные IP-адреса клиентам через протокол DHCP.
Динамическое распределение: DHCP-сервер производит динамическую раздачу IP-адреса клиенту. Этот механизм распределения может назначить постоянный IP-адрес или IP-адрес с ограниченным сроком пользования для клиента. Когда время аренды адреса истекает, клиент должен повторно запросить IP-адрес. Сетевой администратор может выбирать для каждого клиента свой механизм распределения по протоколу DHCP.

5.3.1. Настройка сервера DHCP

5.3.1.1. Введение

Сервер DHCP является поставщиком услуг DHCP. Он использует сообщения DHCP для связи с клиентом DHCP, для того чтобы назначить подходящий IP адрес клиенту, а также, по мере необходимости, назначить другие сетевые параметры клиенту. Сервер DHCP обычно используется для распределения IP адресов при следующих условиях:

- Большой масштаб сети. Слишком сложно вручную осуществить конфигурацию сети, сложно управлять такой сетью.
- Количество хостов превышают число назначаемых IP адресов и невозможно назначить фиксированный IP адрес для каждого хоста.
- Только несколько хостов в сети нуждаются в фиксированных IP адресах.

5.3.1.2. Пул адресов DHCP

DHCP-сервер выбирает IP адрес из пула адресов и передает его вместе с другими параметрами клиенту. Последовательность выделения IP адресов следующая:

1. IP адрес, статически связанный к MAC адресу клиента или идентификатор порта, подключенный к серверу.
2. IP адрес, который записан на сервере DHCP, когда-либо был выделен клиенту.
3. IP адрес, который указан в запросе, полученном от клиента.
4. Первый доступный IP адрес, найденный в пуле адресов.
5. Если нет доступного IP адреса, проверяется IP адрес, срок действия которого истекает, и у которого были конфликты в процессе использования. Если такой IP адрес найден, он присваивается клиенту. Если нет, то не происходит никакого процесса.

5.3.1.3. Настройка через WEB-интерфейс

1. Включение сервера DHCP

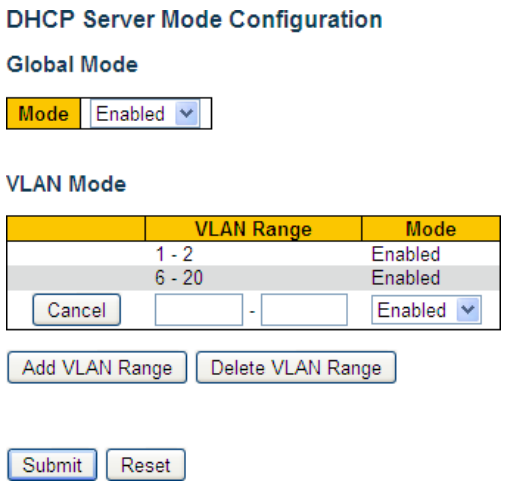


Рис. 34. Включение сервера DHCP

Статус сервера DHCP (Global Mode)
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: выбор данного коммутатора в качестве сервера DHCP для назначения клиенту IP адреса.
Режим работы сервера и диапазон VLAN ({VLAN Range, Mode})
Диапазон настройки: {1~4095, Disabled/Enabled} ((Включить/Выключить)
Функция: если для клиента VLAN, который обращается за IP-адресом, установлено значение «Enable», DHCP-сервер выделяет IP-адрес клиенту. В противном случае DHCP-сервер не выделяет клиенту IP-адрес.

2. Создание пула адресов DHCP

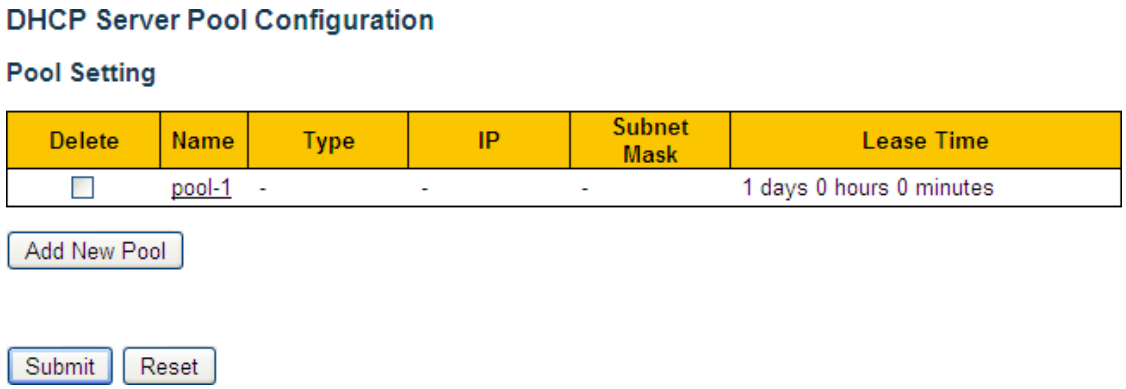


Рис. 35. Создание пула адресов DHCP

Имя (Name)
Настраиваемый диапазон: 1~32 символов;
Описание: настройка имени пула IP-адресов.
Нажмите <Add New Pool> для создания нового пула адресов DHCP.

3. Для настройки пула IP-адресов DHCP необходимо нажать на его имя (<Name>, см. рис.35). После этого появится окно настройки (рис. 36).

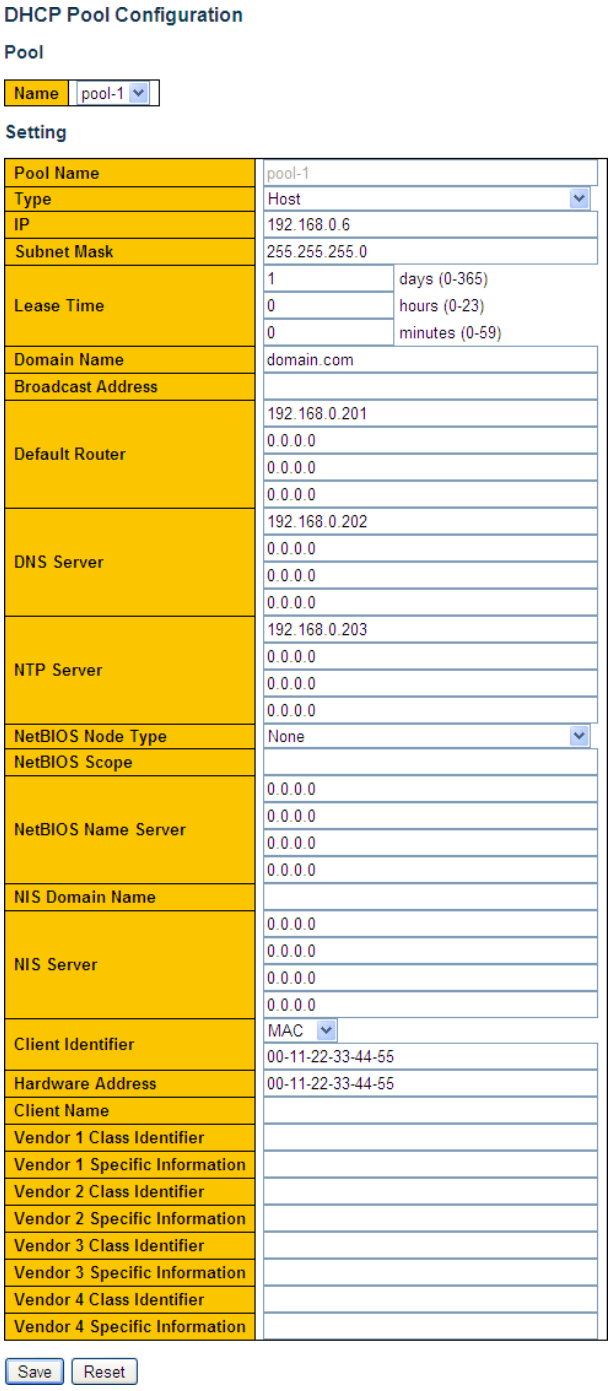


Рис. 36. Создание пула адресов DHCP

Имя (Name)

Функция: выбор созданного имени пула.

Тип (Type)

Опции: None/Network/Host (Нет/Сеть/Хост).

Значение по умолчанию: None (Нет)

Функция: Настройка типа пула адресов. «Network» - коммутатор динамически выделяет IP-адреса нескольким DHCP-клиентам. «Host» - коммутатор поддерживает статическое назначение IP-адресов специальным DHCP-клиентам.

IP-адрес, маска подсети ({IP, Subnet Mask})

Функция: «Network» означает, что вы можете настроить диапазон пула IP-адресов, а диапазон адресов определяется маской подсети. Маска подсети - это число длиной 32 бита, состоящее из строки 1 и строки 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Это значение обычно настроено как 255.255.255.0.

«Host» означает, что вы можете настроить ограниченный статический IP-адрес клиента. Распределение статических IP-адресов осуществляется путем ограничения MAC-адреса и IP-адреса клиента. Когда клиент с этим MAC-адресом запрашивает IP-адрес, DHCP-сервер находит IP-адрес, соответствующий MAC-адресу клиента, и выделяет IP-адрес клиенту. Приоритет этого режима распределения выше, чем у динамического распределения IP-адресов, и срок действия адреса является постоянным.

Время действия IP адресов (Lease Time)

Настраиваемый диапазон: 0 дней, 0 часов, 0 минут ~ 365 дней, 23 часа, 59 минут.

Значение по умолчанию: 1 день, 0 часов, 0 минут.

Описание: настройка тайм-аута динамического выделения адресов. Для разных пулов адресов DHCP-сервер может устанавливать разное время действия адресов, но адреса в одном пуле адресов DHCP имеют одинаковое время действия.

Имя домена (Domain Name)

Настраиваемый диапазон: 1 ~ 36 символов.

Функция: настройка доменного имени пула IP-адресов. При назначении IP-адреса клиента нужно присвоить ему также доменное имя.

Широковещательный адрес (Broadcast Address)

Формат: A.B.C.D

Функция: настройка широковещательного адреса клиента.

Роутер по умолчанию (Default Router)

Формат: A.B.C.D

Функция: настройка адреса клиентского шлюза.

Описание: когда DHCP-клиент подключается к хосту, который находится в другом сегменте, данные должны пересылаться через шлюзы. Когда DHCP-сервер выделяет IP-адреса клиентам, он может одновременно указать адреса шлюзов. Для пула адресов DHCP может настроить максимум 4 шлюза.

Сервер DNS (DNS Server)

Формат: A.B.C.D

Функция: настройка адреса клиентского DNS-сервера.

Описание: при подключении к хосту через доменное имя, требуется преобразование доменного имени в IP-адрес. Это действие реализуется с помощью системы доменных имен DNS (Domain Name System). Чтобы разрешить DHCP-клиенту подключиться к хосту через доменное имя, DHCP-сервер может не только выделять IP-адреса клиентам, но и одновременно указывать IP-адреса серверов доменных имен. Пул DHCP-адресов может настраивать до 4-х DNS-серверов.

Сервер NTP (NTP Server)

Формат: A.B.C.D

Функция: настройка адреса сервера DNS.

Тип узла NetBIOS (NetBIOS Node Type)

Опции: None/B-node/P-node/M-node/H-node (B-узел/P-узел/M-узел/H-узел).

Значение по умолчанию: None (Нет)

Функция: настройка типа клиентского узла NetBIOS. Когда клиент DHCP для связи по сети использует протокол NetBIOS, необходимо установить соответствие между именем хоста и IP-адресом, т.е. настроить порядок и метод, которые использует клиент при преобразовании имен NetBIOS в IP-адреса. Различные типы узлов эту информацию в разных режимах.

B-узел использует широковещательные рассылки. P-узел использует сервер имен NetBIOS, отправляя одноадресный пакет для связи с WINS-сервером. M-узел объединяет B-узел и P-узел, но по умолчанию функционирует как B-узел и отправляет первый широковещательный пакет. Если M-узел не может разрешить имя с помощью широковещательной рассылки, он использует P-узел сервера имен NetBIOS, отправляя одноадресный пакет для связи с WINS-сервером во второй раз. H-узел объединяет P-узел и B-узел, но по умолчанию функционирует как P-узел. Если H-узел не может разрешить имя с помощью сервера имен NetBIOS, используется широковещательная рассылка имени.

Контекст NetBIOS (NetBIOS Scope)

Настраиваемый диапазон: 1 ~ 36 символов.

Функция: настройка имени NetBIOS.

Имя сервера NetBIOS (NetBIOS Name Server)

Формат: A.B.C.D.

Функция: настройка адреса WINS-сервера.

Описание: для клиента, работающего под управлением операционной системы (ОС) Microsoft Windows, сервер Windows Internet Naming Service (WINS) предоставляет услугу преобразования имени хоста в IP-адрес того хоста, который использует для связи протокол NetBIOS. Поэтому большинству клиентов на базе ОС Windows требуется настройка WINS. Чтобы разрешить DHCP-клиенту преобразовывать имя хоста в IP-адрес, укажите адрес WINS-сервера, когда DHCP-сервер выделяет IP-адрес клиенту. Пул адресов DHCP позволяет настроить до 4 серверов WINS.

Доменное имя NIS (NIS Domain Name)

Настраиваемый диапазон: 1 ~ 36 символов.

Функция: настройка доменного имени NIS.

Сервер NIS (NIS Server)

Формат: A.B.C.D.

Функция: настройка адреса сервера NIS.

Идентификатор клиента (Client Identifier)

Опции: None/FQDN*/MAC.

Значение по умолчанию: None (Нет)

Функция: если тип пула - хост, необходимо указать уникальный идентификатор клиента.

* FQDN - полное доменное имя (англ. «Fully Qualified Domain Name» или FQDN, дословно: полностью определенное имя домена) – имя, однозначно определяющее узел в сети.

Аппаратный адрес (Hardware Address)
Формат: HH-HH-HH-HH-HH-HH (H - шестнадцатеричное число).
Функция: если тип пула - хост, необходимо настроить ограниченный статический MAC-адрес клиента.
Имя клиента (Client Name)
Настраиваемый диапазон: 1 ~ 36 символов.
Функция: настройка имени пользователя клиента.
Идентификаторы класса вендора (Vendor N Class Identifier)
Настраиваемый диапазон: 1 ~ 64 символов.
Функция: настройка идентификатора класса вендора.
Идентификаторы класса вендора (Vendor N Class Identifier)
Настраиваемый диапазон: 1 ~ 64 символов (шестнадцатеричные числа).
Функция: настройка информации о вендоре.

4. Настройка исключений IP-адресов (IP-адреса не выделяются динамически в пуле адресов DHCP).

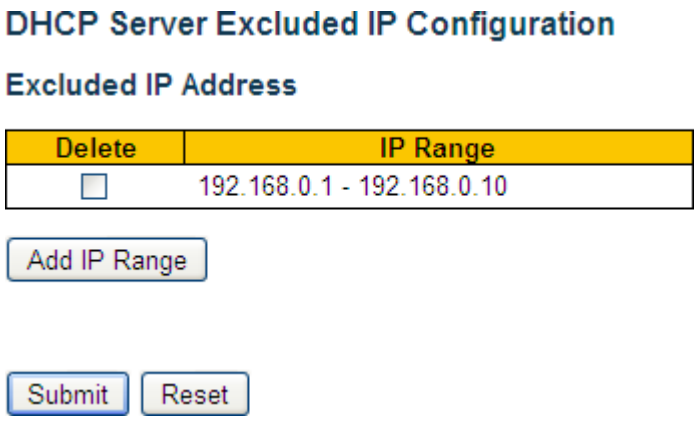
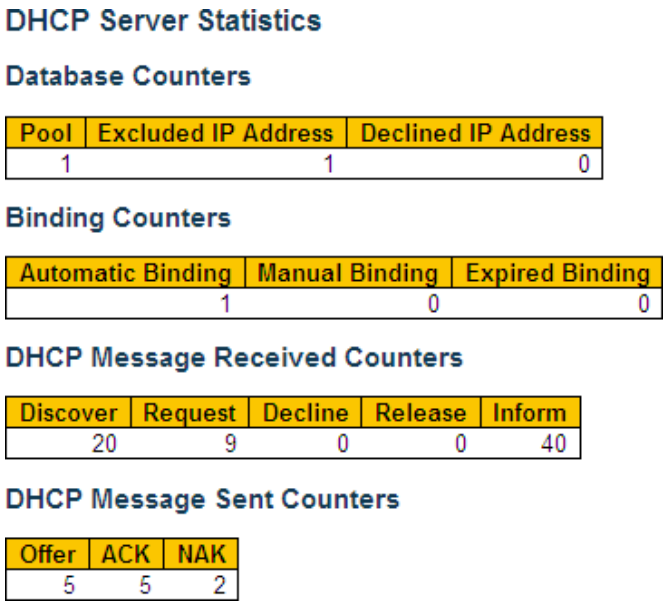


Рис. 37. Настройка исключений IP-адресов

Диапазон IP-адресов (IP Range)
Функция: настройка диапазона IP-адресов, которые не выделяются динамически в пуле адресов DHCP. При назначении IP-адресов DHCP-сервер должен исключить занятый IP-адрес (например, IP-адреса шлюза и DNS-сервера). В противном случае один и тот же IP-адрес может быть назначен двум клиентам, что приведет к конфликту IP-адресов.
Чтобы настроить диапазон IP-адресов, которые не выделяются динамически, нажмите <Add IP Range>.

5. Отображение статистики сервера DHCP.



DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
1	1	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
1	0	0

DHCP Message Received Counters

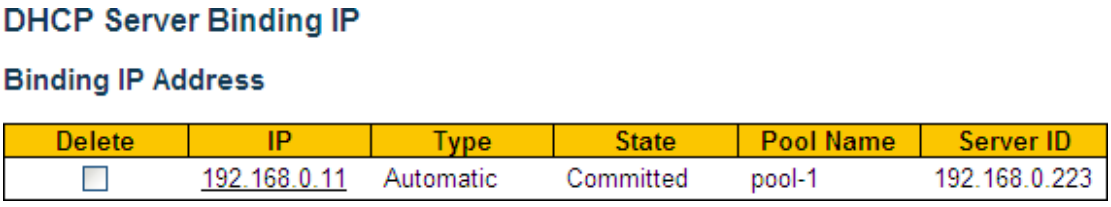
Discover	Request	Decline	Release	Inform
20	9	0	0	40

DHCP Message Sent Counters

Offer	ACK	NAK
5	5	2

Рис. 38. Статистика сервера DHCP

6. Просмотр информации об IP-адресах, выделенных DHCP-сервером.



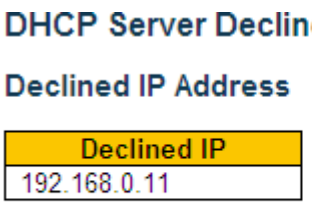
DHCP Server Binding IP

Binding IP Address

Delete	IP	Type	State	Pool Name	Server ID
☐	192.168.0.11	Automatic	Committed	pool-1	192.168.0.223

Рис. 39. Информация об IP-адресах

7. Просмотр IP-адресов, отклоненных DHCP-клиентами



DHCP Server Declined IP

Declined IP Address

Declined IP
192.168.0.11

Рис. 40. Информация об IP-адресах

Когда клиент обнаруживает, что IP-адрес, выделенный сервером, конфликтует со статическим IP-адресом в том же сегменте сети, он отправляет на сервер пакет отклонения, чтобы отклонить этот IP-адрес. Сервер записывает IP-адрес, отклоненный клиентом, и не будет выделять этот IP-адрес другим клиентам в течение определенного периода времени.

5.3.1.4. Пример типовой настройки

Как показано на рисунке 41, коммутатор A работает как DHCP-сервер, а коммутатор B - как DHCP-клиент. Порт 3 коммутатора A соединяется с портом 4 коммутатора B. Клиент отправляет сообщения с запросом IP-адреса, и сервер может назначить IP-адрес клиенту двумя способами. Диапазон исключенных IP-адресов составляет 192.168.0.1~192.168.0.10, в том случае, если DHCP-сервер динамически выделяет IP-адрес.

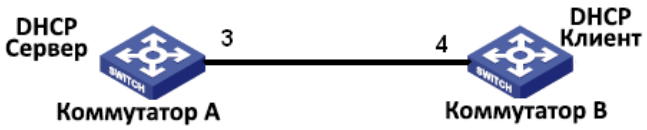


Рис. 41. Пример типовой настройки DHCP

Статические IP-адреса:

1. Настройка коммутатора A:
   - установите статус сервера DHCP в состояние «Enable» (Включено) в соответствующих VLAN (см. рис. 34);
   - создайте пул IP-адресов DHCP: pool-1, см. рис. 35;
   - установите тип пула как «Host»; IP-адрес 192.168.0.6; маска 255.255.255.0; Свяжите MAC-адрес коммутатора B: 00-11-22-33-44-55 (см. рис. 36);
2. Настройка коммутатора B:
   - Настройте коммутатор на автоматическое получение IP-адреса через DHCP;
   - Коммутатор B получит IP адрес 192.168.0.6 и маску подсети 255.255.255.0 от сервера DHCP (см. рис. 42).

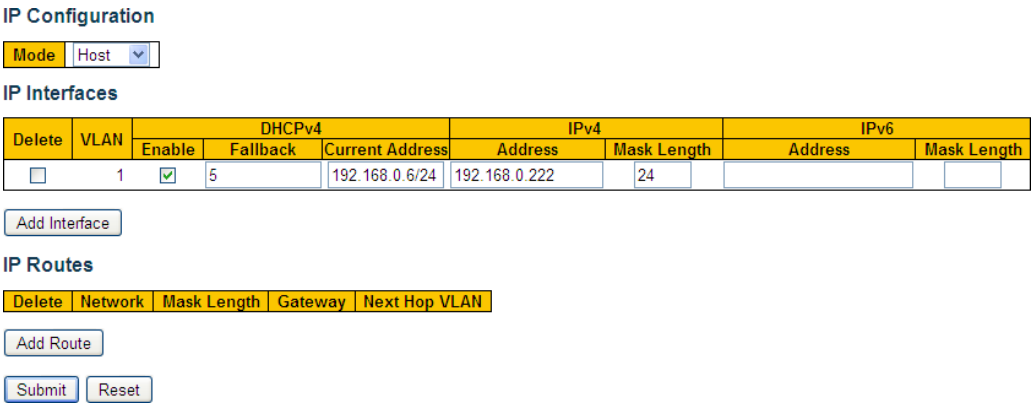


Рис. 42. DHCP-клиент получает IP-адрес-1

Динамические IP-адреса:

3. Настройка коммутатора A:
   - установите статус сервера DHCP в состояние «Enable» (Включено) в соответствующих VLAN (см. рис. 34);
   - создайте пул IP-адресов DHCP: pool-1 (см. рис. 35);

- установите тип пула как «Network»; IP-адрес 192.168.0.6; маска 255.255.255.0; Свяжите MAC-адрес коммутатора B: 00-11-22-33-44-55 (см. рис. 36);

4. Настройка коммутатора B:
   - Настройте коммутатор на автоматическое получение IP-адреса через DHCP;
   - DHCP-сервер по порядку выполняет поиск назначаемых IP-адресов в пуле адресов и выделяет первый найденный IP-адрес, а также другие сетевые параметры для коммутатора B; маска подсети 255.255.255.0 (см. рис. 43).

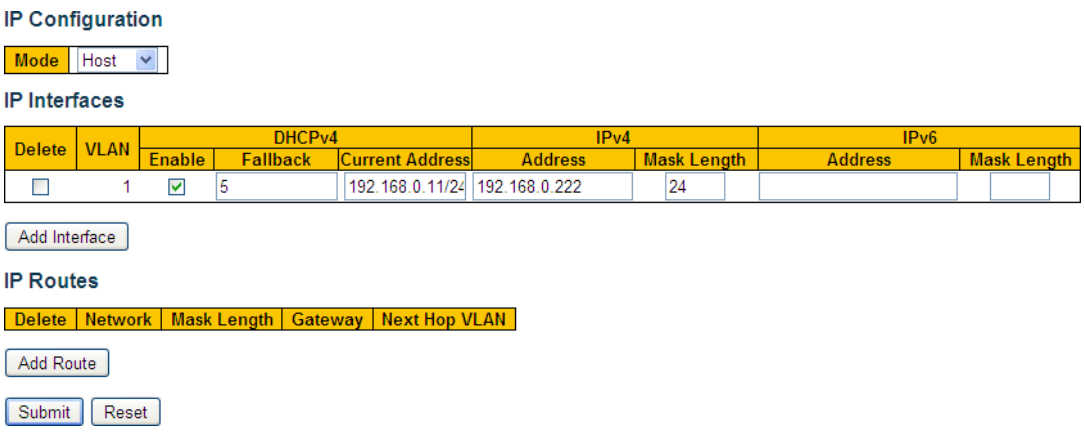


Рис. 43. DHCP-клиент получает IP-адрес-2

5.3.2. DHCP Snooping

5.3.2.1. Введение

DHCP Snooping - это функция мониторинга сервисов DHCP на 2-м уровне, которая также является функцией безопасности DHCP, обеспечивающей безопасность клиента. Механизм безопасности DHCP Snooping осуществляет контроль за тем, чтобы только доверенный порт мог перенаправить сообщение с запросом клиента DHCP на действительный сервер. Кроме того DHCP Snooping может контролировать источник ответного сообщения сервера DHCP, гарантируя клиенту получение IP адреса от действительного сервера, предотвращая назначения IP адресов или параметров конфигурации другим хостам от поддельных или недопустимых серверов DHCP.
Механизм безопасности DHCP Snooping делит порты на доверенные и не доверенный (не надежный).

- Доверенный порт: это порт, который подключается к действительному серверу DHCP. Доверенный порт обычно перенаправляет сообщения с запросом клиентов DHCP и ответные сообщения серверов DHCP, чтобы клиенты DHCP могли получать действительные IP адреса гарантированно.
- Не доверенный порт: это порт, который подключен к недействительному серверу DHCP. Не доверенный порт не перенаправляет сообщения с запросом клиентов DHCP и ответные сообщения серверов серверов DHCP, чтобы клиенты DHCP не получали недействительные IP адреса.

5.3.2.2. Настройка через WEB-интерфейс

1. Включение функции DHCP Snooping.

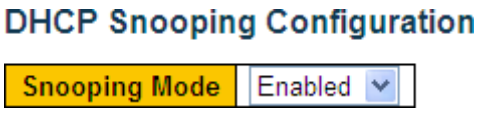


Рис. 44. Статус DHCP Snooping

Режим DHCP Snooping (DHCP Snooping Mode)
Опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Disable (Выключено)
Описание: Включение/Выключение функции DHCP Snooping.

У коммутатора, который работает и как сервер DHCP и как клиент, нельзя включить функцию DHCP Snooping.

2. Настройка доверенных портов

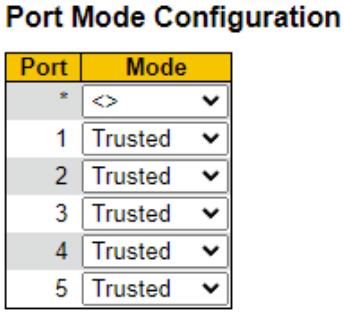


Рис. 45. Статус DHCP Snooping

Режим (Mode)
Опции: Trust/Untrust (Доверенный/Не доверенный)
Значение по умолчанию: Untrust (Не доверенный)
Описание: настройка порта в режимы Доверенный/Не доверенный. Порты, которые подключаются к действительным серверам DHCP напрямую или косвенно, являются доверенными портами.

Настройка порта как доверенного и назначение его транковым портом (Port Trunk) являются взаимоисключающими. Порт, принадлежащий транковой группе, нельзя настроить как доверенный порт. Доверенный порт не может быть присоединен к транковой группе.

5.3.2.3. Пример типовой настройки

Как показано на рис. 46, клиент DHCP запрашивает IP адрес у сервера DHCP. В сети присутствует недействительный сервер DHCP. Настройте порт 1 как доверенный с помощью функции DHCP Snooping, чтобы можно было переслать сообщение с запросом клиента DHCP на сервер DHCP и направить ответное сообщение сервера DHCP клиенту DHCP. Установите порт 3 как не доверенный (не надежный), который не сможет переслать сообщение с запросом клиента DHCP и получить ответное сообщение недействительного сервера DHCP, чтобы гарантировать клиенту получение действительного IP адреса от действительного сервера DHCP.

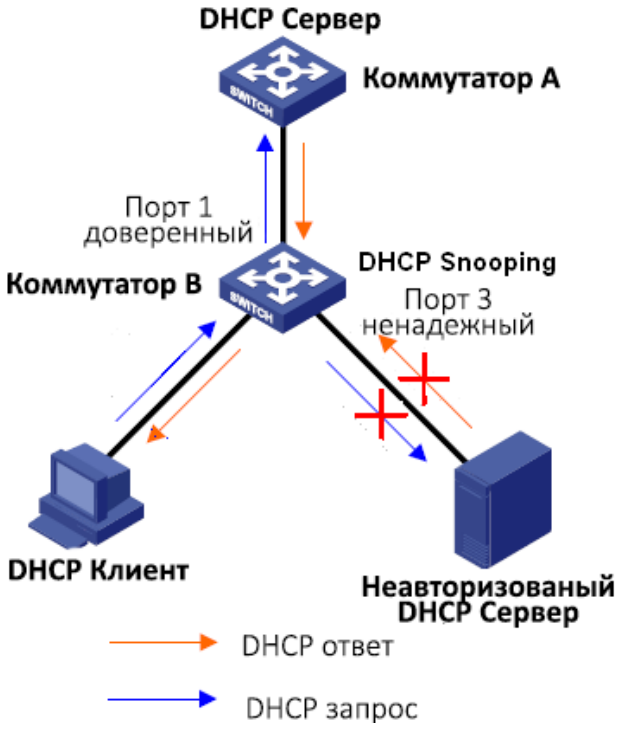


Рис. 46. Пример типовой настройки DHCP Snooping

Настройка коммутатора B:

- Включите функцию DHCP Snooping, см. рис. 44;
- Настройте порт 1 коммутатора B как доверенный (Trust), а порт 3 настройте как ненадежный (Untrust), см. рис. 45.

5.3.3. Функция Option 82 DHCP

Функция Option 82 (Relay Agent Information Entry) обеспечивает запись информации о клиенте. Когда DHCP Snooping с поддержкой Option 82 получает сообщение с запросом от клиента DHCP, он добавляет соответствующее поле Option 82 в сообщение, а затем передает сообщение на сервер DHCP. Сервер, поддерживающий Option 82, может гибко распределять адреса в соответствии с сообщением Option 82. После того, как функция Option 82 была включена, в сообщение необходимо добавить поле Option 82. Поле Option 82 коммутаторов данной серии содержит два подпараметра: вспомогательную опцию 1

(Circuit ID, идентификатор порта запроса) и вспомогательную опцию 2 (Remote ID, идентификатор самого DHCP). Ниже представлены форматы этих двух подпараметров:

- Подпараметр 1 содержит идентификатор VLAN и номер порта, который получает сообщение с запросом от клиента DHCP.

Табл. 2

Формат полей подпараметра 1:

Тип подпараметра (0x01)	Длина (0x04)	VLAN ID	Номер порта
Один байт	Один байт	Два байта	Два байта

Тип подпараметра: тип подпараметра 1-й из 1-го;
Длина: количество байтов, которые занимают идентификатор VLAN и номер порта;
VLAN ID: на устройстве с включенной функцией DHCP Snooping - идентификатор VLAN порта, который получает сообщение с запросом от клиента DHCP;
Номер порта: на устройстве с включенной функцией DHCP Snooping - номер порта, который получает сообщение с запросом от клиента DHCP.

- Содержимым подпараметра 2 является MAC-адрес устройства с функцией DHCP Snooping, которое получает сообщение с запросом от клиента DHCP или строку символов, настроенную пользователями (см. табл. 3).

Табл. 3

Формат полей MAC адреса подпараметра 2:

Тип подпараметра (0x02)	Длина (0x06)	MAC адрес
Один байт	Один байт	6 байт

Тип подпараметра: тип подпараметра 2-й из 2-х;
Длина: количество байтов, которые занимают содержимое подпараметра 2; MAC-адрес занимает 6 байтов, а строка символов занимает 16 байт;
MAC-адрес: содержимое подпараметра 2 является MAC-адресом устройства с функцией DHCP Snooping, которое получает сообщение с запросом от клиента DHCP.

5.3.3.1. DHCP Snooping с поддержкой функции Option 82

1. Введение

Если устройство с функцией DHCP Snooping поддерживает функцию Option 82, то когда DHCP Snooping получает сообщение с запросом DHCP, оно обрабатывает это сообщение в соответствии с тем, содержит ли сообщение Option 82 и политику клиента, а затем перенаправляет обработанное сообщение на сервер DHCP. Метод обработки показан в таблице 4:

Получение сообщения с запросом от клиента DHCP	**Конфигурационная политика**	**Обработка сообщения с запросом устройством с DHCP Snooping**
Сообщение с запросом содержит поле Option 82	Отбрасывание	Отбросить запрос
	Удержание	Сохранить формат сообщения без изменений и переслать

	Замещение	Заменить поле Option 82 в сообщении полем Option 82 устройства Snooping и переслать новое сообщение
Сообщение с запросом не содержит поле Option 82	Отбрасывание/ Сохранение/ Замещение	Добавить в сообщение поле Option 82 устройства Snooping и переслать его

Когда устройство с функцией DHCP Snooping получает ответное сообщение от сервера DHCP, и если сообщение содержит поле Option 82, поле Option 82 удаляется, ответное сообщение обрабатывается и направляется клиенту.

2. Настройка через WEB-интерфейс
Настройка DHCP Snooping Option 82:

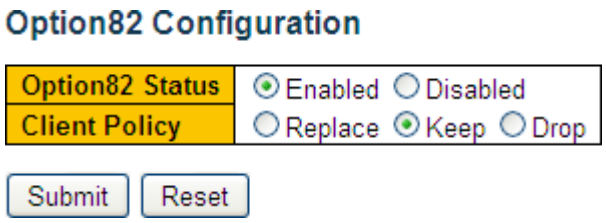


Рис. 47. Настройка функции Option 82 на устройстве с DHCP Snooping

Статус Option 82 (Option 82 Status)
Опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Disable (Выключено)
Функция: Включение/Выключение функции Option 82 на устройстве с DHCP Snooping.
Политика клиента (Client Policy)
Опции: Drop/Replace/Keep (Отбрасывание/Замещение/Сохранение)
Значение по умолчанию: Replace (Замещение)
Функция: Настройка политики клиента. Устройство с функцией DHCP Snooping обрабатывает сообщение с запросом, отправленное от клиента в соответствии с политикой клиента (см. табл. 4).

6. Часы

6.1. Настройка часов

1. Настройка часового пояса

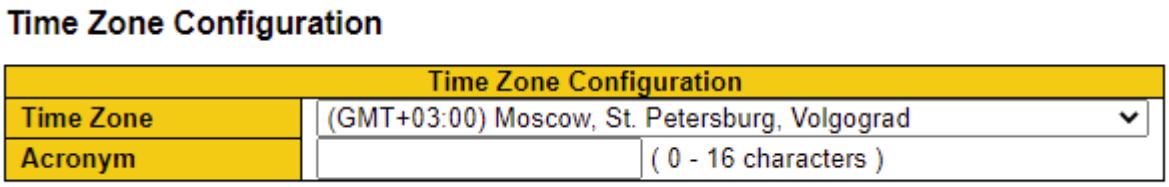


Рис. 48. Настройка часового пояса

Часовой пояс (Time Zone)
Функция: Выбор часового пояса.
Акроним (Acronym)
Функция: Описание часового пояса.

6.2. Протокол SNTP

Протокол SNTP (Simple Network Time Protocol) обеспечивает синхронизацию времени между сервером и клиентом путём запросов и ответов. Если коммутатор выступает в качестве клиента, он синхронизирует своё время со временем сервера.

- Для синхронизации времени по SNTP должен существовать активный сервер SNTP.
- Вся информация о времени, передаваемая в протоколе SNTP, является стандартной информацией о времени для часового пояса 0.

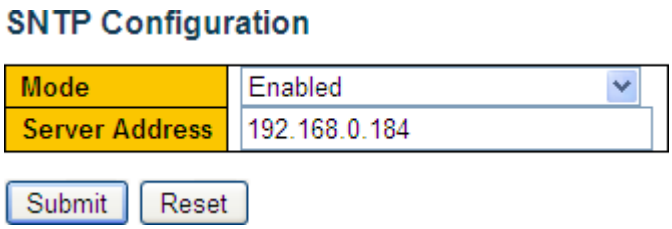


Рис. 49. Настройка часового пояса

Статус SNTP (Mode)
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: Включение или выключение SNTP.
Адрес сервера (Server IP)
Формат: A.B.C.D
Описание: Настройка IP адреса сервера SNTP. Клиенты будут синхронизировать своё время в соответствии с сообщениями этого сервера.
Проверьте, синхронизируются ли время.
Нажмите [Basic Configuration] → [System Information], чтобы просмотреть информацию о времени (см. рис. 52).

System Information

System	
Contact	Symanitron Ltd., phone number +7 499 685 1790; symanitron.ru
Name	SWITCH
Location	111674 Moscow Russia 17 Rudnevka street
Hardware	
Device Type	SEWM10A-1S4T
Device MAC Address	48-be-2d-00-49-54
S/N	S30U0039A220100264
Time	
System Date	1970-01-01T00:40:03+00:00
System Uptime	0d 00:40:03
Software	
Software Version	R1001
Code Date	Apr 23 2020 11:25:57
Code Revision	Build-24.0.98.1
Hardware Version	V2.1
Logic Version	V3.0.0

Рис. 50. Просмотр информации о дате и времени

7. Настройка портов

1. При помощи функции конфигурации портов можно настроить скорость порта (port speed), статус порта (port status), тип управления потоком (flow control) и другие параметры:

Port Configuration

Port	Alias	Link	Media-Type		Speed		Adv Duplex		Adv Speed			Flow Control			Maximum Frame Size	Reset
			Type	Configured	Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx		
*				<>		<>	☑	☑	☑	☑	☐	☐			9600	☐
1	1		FE	copper	Down	Auto	☑	☑	☑	☑	☐	☐	✕	✕	9600	☐
2	2		FE	copper	Down	Auto	☑	☑	☑	☑	☐	☐	✕	✕	9600	☐
3	3		FE	copper	100fdx	Auto	☑	☑	☑	☑	☐	☐	✕	✕	9600	☐
4	4		FE	copper	Down	Auto	☑	☑	☑	☑	☐	☐	✕	✕	9600	☐
5	5		FX	fiber	Down	100Mbps FDX	☐	☐	☐	☐	☐	☐	✕	✕	9600	☐

Submit Reset

Рис. 57. Настройка портов

Статус соединения (Link)

Функция: отображение текущего статуса соединения на порту.

Green (зеленый): порт находится в состоянии LinkUp, т.е. в состоянии соединения.

Red (красный): порт находится в состоянии LinkDown, т.е. на порту соединения нет.

Скорость и тип подключения (Speed-Current)

Функция: отображение текущей скорости портов в состоянии LinkUp, т.е в состоянии соединения, а также отображение способа связи на порту (Full-duplex или Half-duplex).

Скорость порта (Speed-Configured)

Опции: Disabled/Auto/10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX/1Gbps FDX (Отключен/Авто/10Мб/с, полудуплкес/10Mbps, FDX/100Мб/с, полудуплекс/100Мб/с, дуплекс/1Гб/с, дуплекс).

Значение по умолчанию: Auto (Авто)

Функция: настройка скорости и режима работы портов. Disabled (Отключен) означает, что порт отключен и передача данных невозможна. Этот значение физически отключает порт и выдается аварийная сигнализация на порту.
Описание: скорость и режим работы портов могут быть согласованы автоматически или установлены принудительно. Когда установлено значение Auto (Авто), скорость порта и режим работы будут согласованы автоматически в соответствии с состоянием подключения порта к источнику данных. Рекомендуется включить автосогласование для каждого порта, чтобы избежать проблем с подключением, вызванных несоответствующей конфигурацией порта. Если вы хотите принудительно установить скорость порта и режим работы, убедитесь, что на подключенных портах на обоих сторонах линии связи одинаковая конфигурация скорости и режима.

- Порты 10/100Base-TX могут быть настроены в режиме Auto, а также в режимах 10Мбит/с, полудуплекс/10Мбит/с, дуплекс/100Мбит/с, полудуплекс/100Мбит/с, дуплекс.
- Порты 10/100/1000Base-TX могут быть настроены в режиме Auto, а также в режимах 10Мбит/с, полудуплекс/10Мбит/с, дуплекс/100Мбит/с, полудуплекс/100Мбит/с, дуплекс/1 Гб/с, дуплекс.

Автосогласование режима работы (Adv Duplex)
Опции: Fdx/Hdx (Дуплекс/Полудуплекс).
Функция: настройка автосогласования режима работы портов.
Описание: Fdx означает, что порт может принимать и передавать данные одновременно; Hdx означает, что одновременно порт либо принимает, либо передает данные. Когда режим порта установлен в Auto, дуплексный режим порта определяется посредством согласования с удаленным узлом по умолчанию. Согласованный дуплексный режим может быть либо Fdx, либо Hdx.
Автосогласование скорости (Adv Speed)
Опции: 10M/100M/1G (10Мбит/с / 100Мбит/с / 1 Гб/с).
Функция: настройка автосогласования скорости работы портов.
Описание: если для режима порта установлено значение Auto, скорость порта по умолчанию определяется путем согласования с удаленным узлом. Согласованная скорость может быть любой в пределах допустимого диапазона скорости порта. Параметр можно настроить так, чтобы порт согласовывал только некоторые скорости, тем самым управлять согласованием скорости.

Конфигурация «Adv Duplex» и «Adv Speed» работают только в автоматическом режиме.

Управление потоком (Flow Control)
Опции: Enabled/Disabled (Выключено/Включено).
Значение по умолчанию: Disabled (Выключено).
Функция: Включить/Выключить режим управления потоком для определенного порта.

Описание: После того, как функция управления потоком (Flow Control) будет включена, порт сообщит отправителю о замедлении скорости передачи, чтобы избежать потери пакетов в соответствии с каким-либо алгоритмом или протоколом, в том случае, если поток, полученный портом больше, чем размер кэша порта. Настройка режимов управления потоком для устройств, работающих по разным типам способа связи (дуплекс/полудуплекс) выполняется разными способами. Для устройств, работающих в полнодуплексном режиме, принимающая сторона должна отправить специальный кадр (Pause frame), чтобы сообщить отправителю о прекращении отправки сообщений. Когда отправитель получит Pause frame, он должен прекратить отправку сообщений на период «времени ожидания» (wait time), указанного в Pause frame и продолжить отправку сообщений после окончания «времени ожидания». Для устройств, работающих в полудуплексном режиме, обеспечивается поддержка режима управления потоком методом обратного давления. Дело в том, что принимающая сторона намеренно создает конфликт или выдает сигнал несущей. Соответственно, когда отправитель обнаруживает конфликт или сигнал несущей, необходима задержка передачи данных.

Curr Rx/Curr Tx

Функция: отображение статуса управления потоком на портах.

Максимальный размер кадра (Maximum Frame Size)

Настраиваемый диапазон: 1518 ~ 9600 байт.

Значение по умолчанию: 9600 байт.

Функция: настройка максимального размера пакета, принимаемого портом. Пакеты, размер которых превышает указанное значение, отбрасываются.

Сброс (Reset)

Опции: Enabled/Disabled (Выключено/Включено).

Значение по умолчанию: Disabled (Выключено).

Функция: Сбросить порт или нет.

2. Отображение статистики портов

Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	2511	2031	482759	880414	0	0	0	0	824
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0

Рис. 58. Статистика портов

Порт (Port)

Нажмите <port> для вывода страницы с детализацией статистики по конкретному порту.

Пакеты (Packets)

Отображение количества пакетов, которые отправляет и получает каждый порт.

Байты (Bytes)

Отображение количества байт, которые отправляет и получает каждый порт.

Ошибки (Errors)

Отображение количества пакетов с ошибками, которые отправляет и получает каждый порт.

Отброс (Drops)

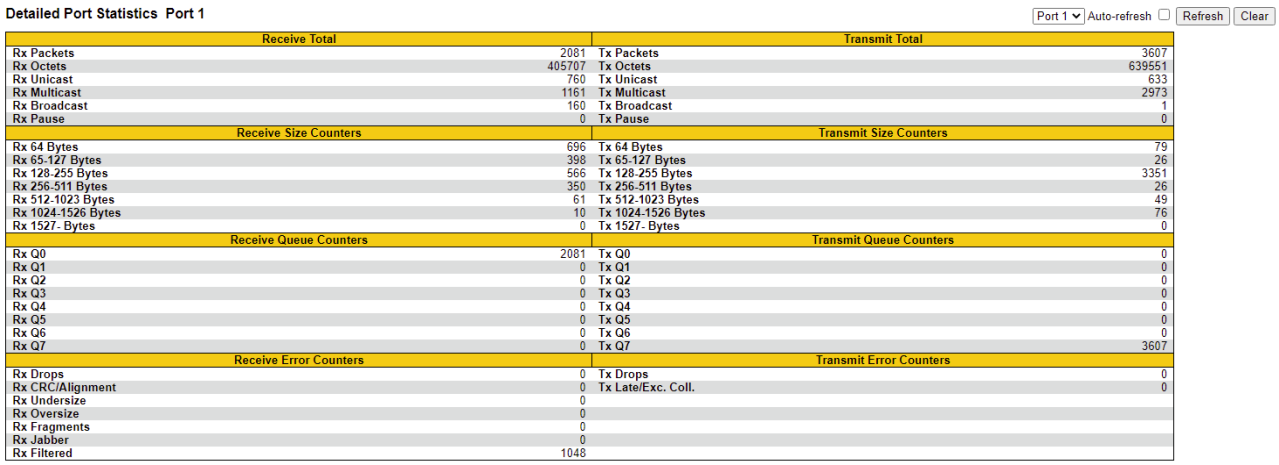
Отображение количества пакетов, которые были отброшены из-за конфликтов приема/передачи данных.

Получено отфильтрованных (Filtered Received)

Отображение количества пакетов, которые были отфильтрованы при приеме данных.

3. Отображение детальной статистики порта

Нажмите <port> для вывода страницы с детализацией статистики по конкретному порту.



Detailed Port Statistics Port 1

Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	2081	Tx Packets	3607
Rx Octets	405707	Tx Octets	639551
Rx Unicast	760	Tx Unicast	633
Rx Multicast	1161	Tx Multicast	2973
Rx Broadcast	160	Tx Broadcast	1
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	696	Tx 64 Bytes	79
Rx 65-127 Bytes	398	Tx 65-127 Bytes	26
Rx 128-255 Bytes	566	Tx 128-255 Bytes	3351
Rx 256-511 Bytes	350	Tx 256-511 Bytes	26
Rx 512-1023 Bytes	61	Tx 512-1023 Bytes	49
Rx 1024-1526 Bytes	10	Tx 1024-1526 Bytes	76
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	2081	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	3607
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	1048		

Рис. 59. Детальная статистика порта

8. Настройка QoS

8.1. Введение

Функция QoS (Quality of Service) позволяет дифференцировать сервисы, в зависимости от разных требований в условиях ограниченной пропускной способности путём контроля трафика и управления потоком трафика в IP сетях. QoS пытается удовлетворить задачи передачи данных различных сервисов, снизить задержки в передачи данных и минимизировать эффект от задержек, в зависимости от приоритета сервиса.

Классификация трафика, контроль трафика, формирование трафика, управление перегрузкой и предотвращение перегрузки являются основной концепцией QoS.

Классификация трафика: идентифицирует объект на основе определенных правил сопоставления. Классификация трафика - основополагающая функция QoS.

Контроль трафика: контролирует скорость трафика пакетов, передаваемых на устройство. Когда скорость трафика превышает указанную скорость, устройство принимает меры ограничения или защиты сетевых ресурсов. Контроль трафика подразделяется на контроль трафика на основе портов и контроль трафика на основе очередей.

Формирование трафика: регулирует скорость рафика. Функция направлена на адаптацию трафика к доступным сетевым ресурсам нисходящего устройства для предотвращения ненужного отбрасывания пакетов и перегрузки. Формирование трафика подразделяется на формирование трафика на основе портов и формирование трафика на основе очередей.
Управление перегрузкой: это обязательно для решения проблемы конкуренции за ресурсы. Управление перегрузкой кэширует пакеты в очередях и определяет последовательность пересылки пакетов на основе определенного алгоритма планирования, обеспечивая предпочтительную пересылку для ключевых служб.
Предотвращение перегрузок: чрезмерное количество задержек передачи данных могут повредить данным, передаваемым через сеть. Функция предотвращения перегрузок следит за использованием всех сетевых ресурсов. При обнаружении повышенного числа задержек, данная функция запускает механизм предупредительного отбрасывания пакетов и изменяет количество передаваемых данных для избавления от перегрузки сети.

8.2. Принцип работы

Каждый порт коммутаторов этой серии поддерживает 8 очередей кэширования от 0 до 7 в порядке возрастания приоритета.
Когда кадр достигает порта, коммутатор определяет очередь для кадра в соответствии с информацией о кадре и данных порта. Коммутаторы этой серии поддерживают классификацию трафика в следующих режимах отображения очереди: порт, информация заголовка 802.1Q, кодовая точка дифференцированных услуг (DSCP) и контрольный список QoS (QCL) с приоритетом в порядке возрастания.
При пересылке данных порт использует режим планирования данных в 8 очередях в соответствии с пропускной способностью каждой очереди. Коммутаторы этой серии поддерживают два режима планирования: 6 взвешенных очередей и SP (строгий приоритет, Strict Priority).
WRR (Weighted Round Robin) планирует потоки данных на основе весового отношения. Очереди получают пропускную способность в зависимости от их весового отношения. WRR отдает приоритет очередям с высоким соотношением веса. Большую полосу пропускания выделяют очередям с более высоким коэффициентом веса.
В режиме SP предпочтительно пересылаются пакеты с высоким приоритетом. Он в основном используется для передачи данных с максимальным приоритетом. Если кадр попадает в очередь с высоким приоритетом, коммутатор прекращает планирование очередей с низким приоритетом и начинает обработку данных очереди с высоким приоритетом. Когда очередь с высоким приоритетом не содержит данных, коммутатор начинает обрабатывать данные очереди с более низким приоритетом.
6-я взвешенная очередь (Queues Weighted) означает, что очередь 6 и очередь 7 используют режим планирования со строгим приоритетом, а очереди 0 ~ 5 используют режим планирования WRR. Данные в очереди 7 обрабатываются до данных в очереди 6. Когда очередь максимального приоритета пуста, устройство переходит к передаче данных следующей по важности очереди и так далее.

8.3. Настройка через Web-интерфейс

1. Настройка режима сопоставления очередей на основе портов.

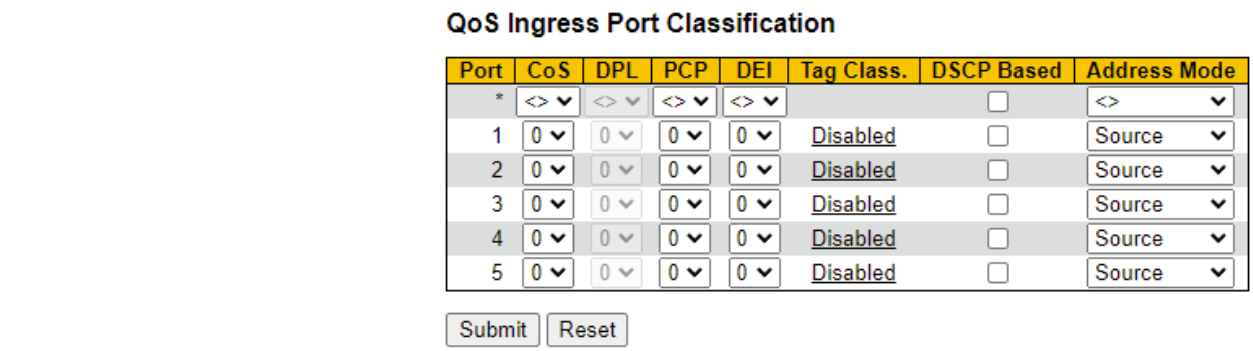


Рис. 60. Настройка QoS

CoS
Настраиваемый диапазон: 0 ~ 7
Значение по умолчанию: 0
Функция: настройка значения порта CoS по умолчанию.
Описание: значение CoS определяет очередь хранения пакетов. Значение CoS находится в диапазоне от 0 до 7, что соответственно соответствует очереди от 0 до 7. После того, как пакет передается на коммутатор, коммутатор присваивает пакету значение CoS. Если полученный тегированный пакет, а классификация тегов отключена, либо полученный пакет не тегированный, значение CoS в пакете является значением CoS по умолчанию для порта, который получает пакет.
PCP
Настраиваемый диапазон: 0 ~ 7
Значение по умолчанию: 0
Функция: настройка значения параметра PCP (Priority Code Point) по умолчанию для порта.
Описание: если пакет не тегированный, приоритет в теге добавляется к пакету, который для порта является значением PCP по умолчанию.
DEI
Настраиваемый диапазон: 0 ~ 1
Значение по умолчанию: 0
Функция: настройка значения параметра DEI (Drop Eligible Indicator) по умолчанию для порта.
Описание: если пакет не тегированный, CFI в теге добавляется к пакету, который для порта является значением DEI по умолчанию.

2. Настройка режима сопоставления очереди на основе заголовка кадра 802.1Q.
Нажмите <Tag Cliass> (см. на рис. 60), чтобы открыть страницу настроек режима сопоставления очереди заголовка кадра 802.1Q (см рис. 61).

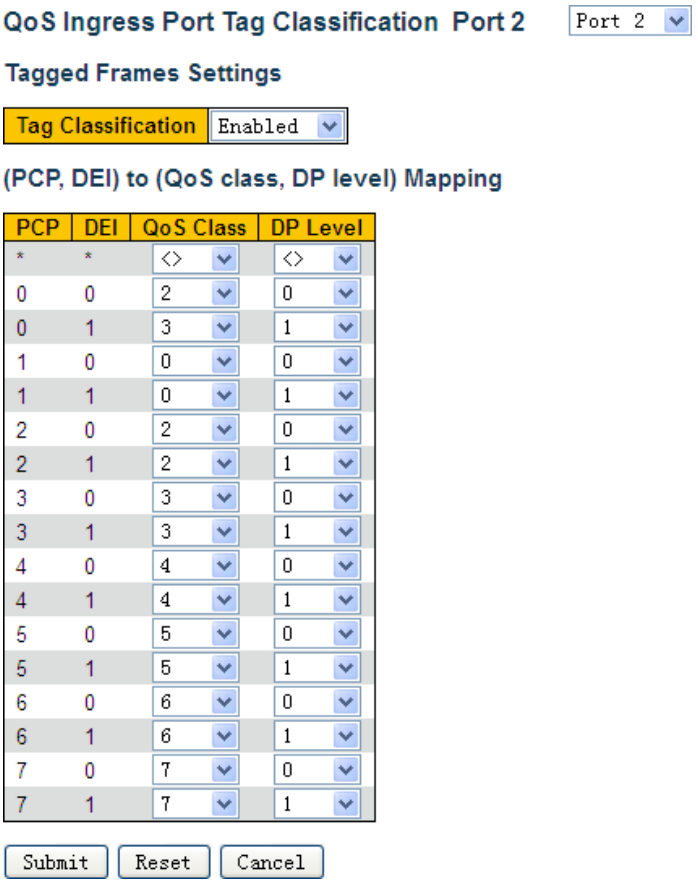


Рис. 61. Настройка режима сопоставления очереди заголовка кадра 802.1Q

Классификация тега (Tag Classification)
Опции: Enabled/Disabled (Выключено/Включено).
Значение по умолчанию: Disabled (Выключено).
Функция: Включение и выключение режима отображения очереди на основе информации заголовка 802.1Q. Этот режим отображения очереди имеет более высокий приоритет по сравнению с режимом отображения очереди на основе портов.

Режим сопоставления очереди на основе информации заголовка 802.1Q применим только к тегированным пакетам, принимаемым портом.

Сопоставление (PCP, DEI) к (класс QoS, уровень DP) ((PCP, DEI) to (QoS class, DP level) Mapping)
Настраиваемый диапазон: 0 ~ 7 (QoS class), 0 ~ 1 (DP Level).
Значение по умолчанию: диапазон значений PCP - 0, 1, 2, 3, 4, 5, 6 и 7, которые соответственно сопоставляются с классами QoS 1, 0, 2, 3, 4, 5, 6 и 7. Значение диапазона DEI составляет 0 и 1, которые соответствуют уровням DP 0 и 1.
Функция: настройка сопоставления (PCP, DEI) к (CoS, DPL) на основе значений PCP и DEI в пакетах данных.
Описание: класс QoS эквивалентен значению CoS. Значение CoS определяет очередь для хранения пакетов, а значения CoS 0-7 соответствуют очередям 0-7. После того, как пакет передан коммутатору, коммутатор назначает пакету значение CoS и DPL. Значение CoS и

значение DPL пакета (CoS, DPL) сопоставляются с (PCP, DEI), если принятый пакет тегированный и включена классификация тегов.
Вы можете выбрать порт для настройки режима сопоставления очереди на основе информации заголовка 802.1Q в правом верхнем углу страницы.

3. Настройка тегирования 802.1p.

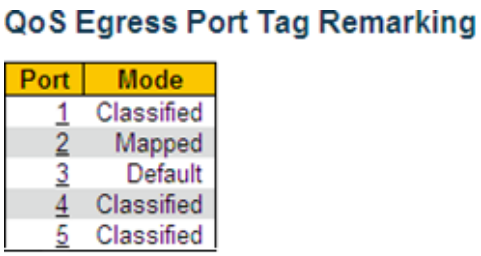


Рис. 62. Настройка тегирования 802.1p

Режим тегирования (Mode)
Опции: Classified/Mapped/Default (Классифицирован/Сопоставлен/По умолчанию)
Функция: режим смены тегов 802.1p, когда исходящий порт пересылает пакеты. Изменение тегов 802.1p используется для обновления значения PCP и значения DEI в пакетах, когда исходящий порт пересылает пакеты.

Если пакеты, пересылаемые исходящим портом, не тегированы, функция смены тегов 802.1p недоступна.

Нажмите <Port>, чтобы перейти на страницу настройки тегирования 802.1p.

1.1. Настройка режима тегирования 802.1p как «Классифицировано» (Classified):

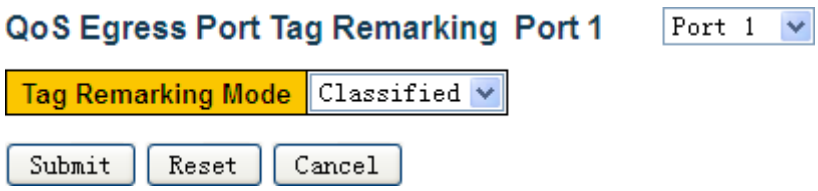


Рис. 63. 802.1p как «Классифицированный» (Classified)

Режим обновления тегов (Tag Remarking Mode)
Опции: Classified/Mapped/Default (Классифицирован/Сопоставлен/По умолчанию)
Значение по умолчанию: Classified (Классифицирован)
Функция: настройка режима тегирования 802.1p как значение «Классифицировано» (Classified): PCP и DEI в пакетах не обновляются, когда исходящий порт пересылает пакеты.
Вы можете выбрать порт для настройки режима смены тегов 802.1p в правом верхнем углу страницы.

1.2. Настройка режима тегирования 802.1p «По умолчанию» (Default):

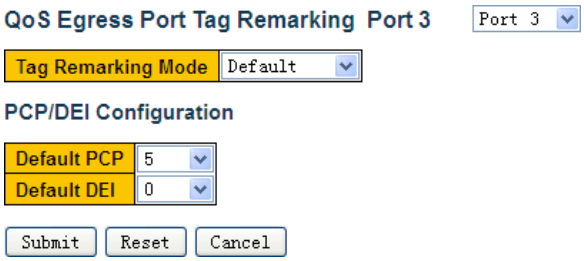


Рис. 64. 802.1p в режиме «По умолчанию» (Default)

Режим обновления тегов (Tag Remarking Mode)
Опции: Classified/Mapped/Default (Классифицирован/Сопоставлен/По умолчанию)
Значение по умолчанию: Classified (Классифицирован)
Функция: настройка режим тегирования 802.1p как значение «По умолчанию» (Default): PCP и DEI в пакетах обновляются до значений по умолчанию (см. значения в нижней части страницы), когда исходящий порт пересылает пакеты.
PCP по умолчанию (Default PCP)
Настраиваемый диапазон: 0 ~ 7
Значение по умолчанию: 0
Функция: настройка значения параметра PCP по умолчанию для исходящего порта.
DEI по умолчанию (Default DEI)
Настраиваемый диапазон: 0 ~ 1
Значение по умолчанию: 0
Функция: настройка значения параметра DEI по умолчанию для исходящего порта.
Вы можете выбрать порт для настройки режима смены тегов 802.1p в правом верхнем углу страницы.
1.3. Настройка режима тегирования 802.1p как «Сопоставлен» (Mapped):

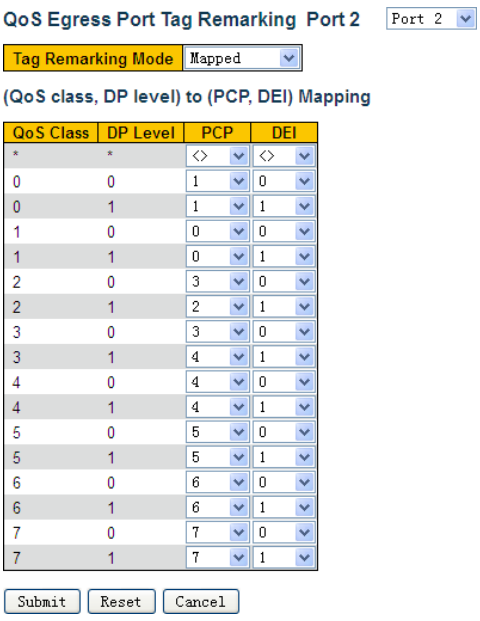


Рис. 65. 802.1p в режиме «Сопоставлен» (Mapped)

Режим обновления тегов (Tag Remarking Mode)
Опции: Classified/Mapped/Default (Классифицирован/Сопоставлено/По умолчанию)
Значение по умолчанию: Classified (Классифицирован)
Функция: настройка режим тегирования 802.1p как значение «Сопоставлен» (Mapped): PCP и DEI в пакетах обновляются до (PCP, DEI), сопоставленного с (CoS, DPL), когда исходящий порт пересылает пакеты. Сопоставление настраивается в нижней части страницы.
Сопоставление (класс QoS, уровень DP) к (PCP, DEI) ((QoS class, DP level) to (PCP, DEI) Mapping)
Настраиваемый диапазон: 0 ~ 7 (PCP), 0 ~ 1 (DEI).
Значение по умолчанию: диапазон классов QoS - 0, 1, 2, 3, 4, 5, 6 и 7, которые, соответственно, сопоставляются со значениями PCP 1, 0, 2, 3, 4, 5, 6 и 7. Диапазон значений DP составляет 0 и 1, которые, соответственно, сопоставляются со значениями DEI 0 и 1.
Функция: настройка сопоставления (CoS, DPL) к (PCP, DEI) на основе значений CoS и DPL в пакетах данных.
Вы можете выбрать порт для настройки режима смены тегов 802.1p в правом верхнем углу страницы.

4. Включение режима сопоставления очередей на основе DSCP.

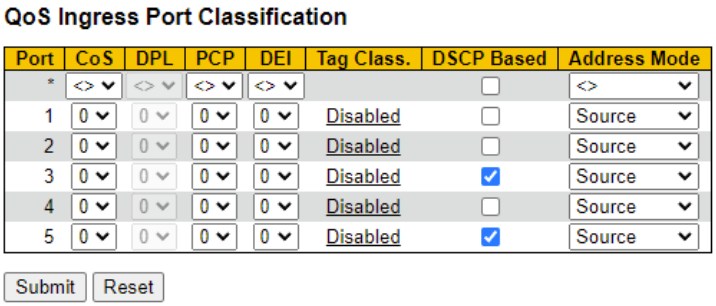


Рис. 66. Режим сопоставления очередей на основе DSCP

Сопоставление на основе DSCP (DSCP Based)
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: включение и выключение режима сопоставления очередей на основе DSCP. Этот DPрежим сопоставления очереди имеет более высокий приоритет по сравнению с режимом сопоставления очереди на основе информации заголовка 802.1Q.

5. Включение преобразования DSCP входящего порта и функции перезаписи DSCP исходящего порта.

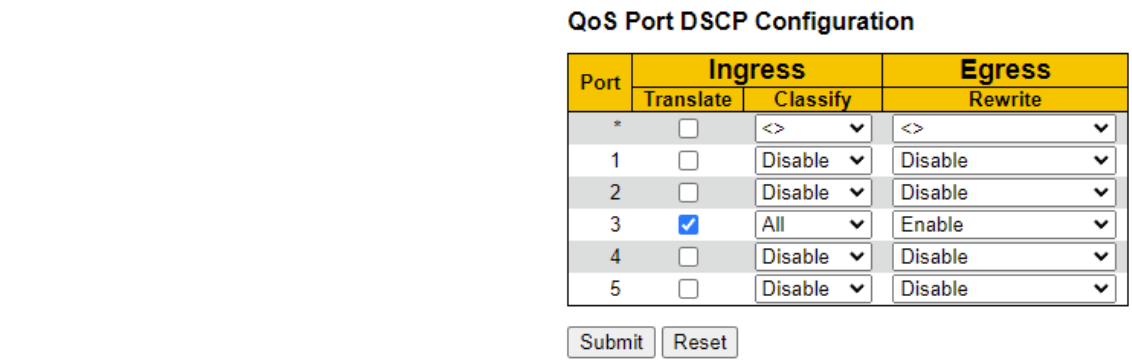


Рис. 67. Настройка функций порта DSCP

Преобразование (Translate)
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: включение и выключение преобразования значения DSCP в пакете, полученном входящим портом. Если установлено значение «Enable», значение DSCP преобразуется в соответствии с таблицей преобразования DSCP (колонка «Translate» на рис. 69).
Классификатор (Classify)
Опции: Disable/DSCP=0/Selected/All (Выключить/ DSCP=0/Выбрано/Все)
Значение по умолчанию: Disable (Выключено)
Функция: если для параметра «Rewrite» задано значение «Enable» выбирается перезаписанное значение DSCP исходящего порта.
Отключить (Disable): значение DSCP в пакетах не перезаписывается, когда исходящий порт пересылает пакеты.
DSCP = 0: если значения DSCP в пакетах равны 0 и исходящий порт пересылает пакеты, значения DSCP в пакетах перезаписываются в соответствии с классификацией на рис. 70.
Выбрано (Selected): если значения DSCP в пакетах являются выбранным значением (колонка «Classify» на рис. 69) и исходящий порт пересылает пакеты, значения DSCP в пакетах перезаписываются.
Все (All): когда исходящий порт пересылает пакеты, значения DSCP в пакетах записываются в соответствии с классификацией (см. рис. 70).
Перезапись (Rewrite)
Опции: Disable/Enable/Remap DP Unaware/Remap DP Aware
Значение по умолчанию: Disable (Выключено)
Функция: настройка режима перезаписи значения DSCP в пакетах, когда исходящий порт пересылает пакеты.
Отключить (Disable): значения DSCP в пакетах не перезаписываются, когда исходящий порт пересылает пакеты.
Включить (Enable): когда исходящий порт пересылает пакеты, возможность перезаписи значений DSCP в пакетах определяется на основе настроек Классификатора (Classify).
Remap DP Unaware: значения DSCP в пакетах перезаписываются на основе сопоставления (столбец «Remap DP0» на рис. 69) из (DSCP, DPL=0) в DSCP, когда исходящий порт пересылает пакеты.

Remap DP Aware: значения DSCP в пакетах перезаписываются на основе сопоставления (колонки «Remap DP0» и «Remap DP1» на рис. 69) из (DSCP, DPL) в DSCP, когда исходящий порт пересылает пакеты.

6. Настройка режима сопоставления очередей на основе DSCP.

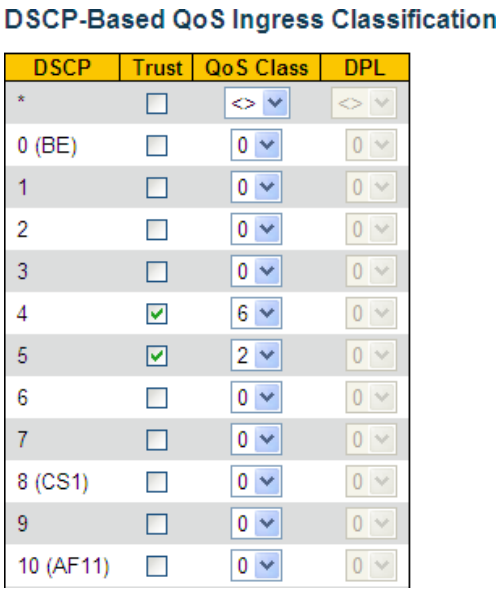


Рис. 68. Настройка режима сопоставления очередей на основе DSCP

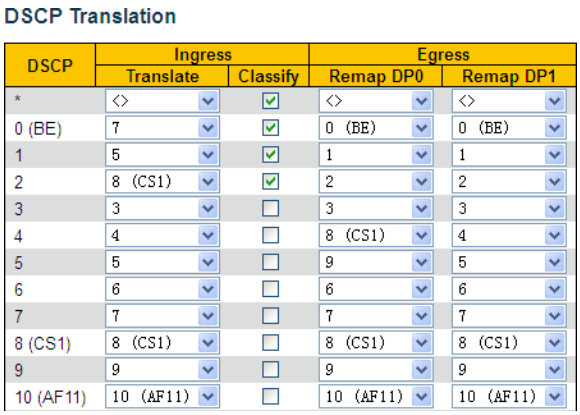
Доверенный режим (Trust)
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: включение и выключение доверенного режима значения DSCP.

Режим сопоставления очередей на основе DSCP применим только к значениям DSCP в пакетах, полученных портом, который является доверенным.

Класс QoS (QoS Class)
Настраиваемый диапазон: 0 ~ 7
Значение по умолчанию: 0
Функция: настройка сопоставленияDSCP к CoS.
Описание: Класс QoS эквивалентен значению CoS. Значение CoS определяет очередь хранения пакетов, а значения CoS 0 ~ 7 соответствуют очередям 0 ~ 7. После того, как пакет со значением DSCP, являющийся доверенным, передан коммутатору, коммутатор выделяет значение CoS в пакете в соответствии с отображением от DSCP к CoS.

Если для входящего порта включен режим «Translate», коммутатор выделяет значение CoS на основе преобразованного значения DSCP. В противном случае коммутатор выделяет значение CoS на основе исходного значения DSCP в пакетах.

7. Настройка режимов преобразования и перезаписи DSCP.


DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	☑	<>	<>
0 (BE)	7	☑	0 (BE)	0 (BE)
1	5	☑	1	1
2	8 (CS1)	☑	2	2
3	3	☐	3	3
4	4	☐	8 (CS1)	4
5	5	☐	9	5
6	6	☐	6	6
7	7	☐	7	7
8 (CS1)	8 (CS1)	☐	8 (CS1)	8 (CS1)
9	9	☐	9	9
10 (AF11)	10 (AF11)	☐	10 (AF11)	10 (AF11)

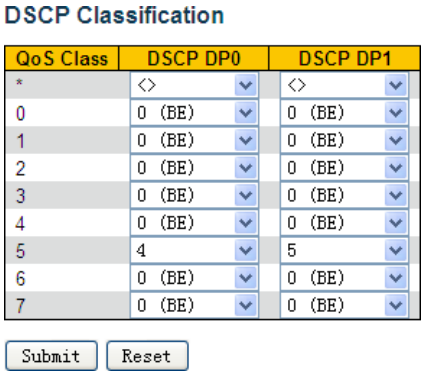
Рис. 69. Настройка режимов преобразования и перезаписи DSCP

Преобразование (Translate)
Настраиваемый диапазон: 0 ~ 63
Функция: настройка таблицы преобразования значений DSCP.
Классификатор (Classify)
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: этот параметр используется для установки выбранного значения DSC, если значение Классификатора (Classify) установлено как «Выбрано» (Selected).

Когда для входящего порта включен режим «Translate», выбранное значение DSCP является значением DSCP после преобразования. В противном случае выбранное значение DSCP является исходным значением DSCP в пакетах.

Remap DP0/ Remap DP1
Настраиваемый диапазон: 0 ~ 63
Функция: настройка согласования от (DSCP, DPL) к значению DSCP.

8. Настройка классификации DSCP.


DSCP Classification

QoS Class	DSCP DP0	DSCP DP1
*	<>	<>
0	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)
5	4	5
6	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)

Submit Reset

Рис. 70. Настройка режимов преобразования и перезаписи DSCP

DSCP DP0/DSCP DP1
Настраиваемый диапазон: 0 ~ 63
Функция: установите сопоставление от (CoS, DPL) к значению DSCP. Класс QoS эквивалентен значению CoS. Значение CoS определяет очередь хранения пакетов, а значения CoS 0-7 соответствуют очередям 0-7.

9. Настройка записей QCL.

QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action						
									CoS	DPL	DSCP	PCP	DEI	Policy	
1	2	Unicast	Any	Any	Any	Any	Any	Any	5	Default	Default	Default	Default	Default	
2	3	Any	Any	Any	10	4-5	Any	Any	6	Default	Default	6	0	Default	
3	4	Any	00-00-00-00-00-23	Any	Any	Any	Any	IPv4	7	1	9	Default	Default	Default	
5	Any	Any	Any	Any	Any	Any	Any	Any	1	Default	Default	Default	Default	Default	
4	Any	Any	Any	Untagged	Any	Any	Any	Any	4	Default	Default	Default	Default	Default	

Рис. 71. Настройка записей QCL

Сопоставление очереди пакетов реализуется путем сопоставления записей QCL. Каждая запись состоит из нескольких условий в отношении логического «И» (AND). Считается, что пакет, полученный портом, соответствует записи QCL только тогда, когда пакет удовлетворяет всем условиям. Записи QCL независимы друг от друга.
Когда имеется несколько записей QCL, устройство сравнивает пакет с записями QCL (одну за другой, сверху вниз). Как только совпадение найдено, выполняется действие, и дальнейшее сравнение не проводится. Нажмите <⊕>, чтобы добавить новую запись QCL; нажмите <ⓔ>, чтобы редактировать запись QCL; нажмите <⊗>, чтобы удалить запись QCL; нажмите <⊙>, чтобы переместить текущую запись вверх; нажмите <⊙>, чтобы переместить текущую запись вниз.
QCE - это идентификатор записи QCL, который нумеруется на основе временной последовательности создания записи.

10. Настройка параметров записей QCL.
10.1. Выбор порта-участника, на котором действует текущая запись QCL.

QCE Configuration

Port Members									
1	2	3	4	5	6	7	8	9	10
☐	☐	☐	☑	☐	☐	☐	☐	☐	☐

Рис. 72. Выбор порта

Порт (Port members)
Функция: выбор порта, на котором действует текущая запись QCL. Все порты по умолчанию являются портами-участниками.

10.2. Настройка параметров записей QCL.

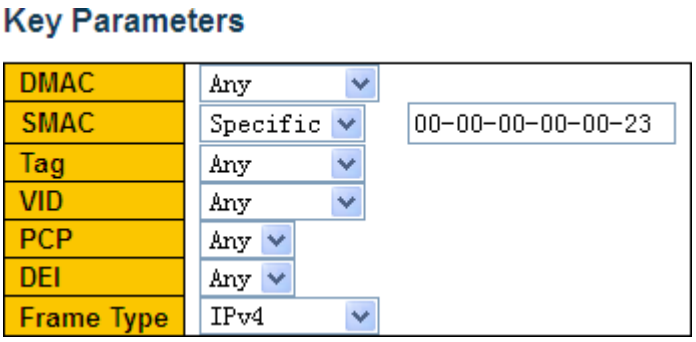


Рис. 73. Настройка параметров записей QCL

DMAC
Опции: Any/Unicast/Multicast /Broadcast
Значение по умолчанию: Any
Функция: установка условий для MAC-адреса назначения. Если MAC-адрес назначения в пакете, полученном портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.
SMAC
Опции: Any/Specific
Значение по умолчанию: Any
Функция: установка условий для MAC-адреса источника. Если установлено значение «Specific», необходимо назначить MAC-адрес. Когда исходный MAC-адрес в пакете, полученном портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.
Tag
Опции: Any/Untagged/Tagged
Значение по умолчанию: Any
Функция: установка условий тегированных пакетов. Когда пакет, полученный портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.
VID
Опции: Any/Specific (1 ~ 4095)/Range (1 ~ 4095)
Значение по умолчанию: Any
Функция: установка условий для VID. Если установлено значение «Specific», необходимо установить значение VID. Когда его значение установлено как «Range», необходимо установить диапазон VID. Когда VID в пакете, полученном портом-участником, соответствует настройкам этого параметра, условие выполняется успешно. Этот параметр недоступен, если для параметра «Tag» установлено значение «Untagged».
VID
Опции: Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7
Значение по умолчанию: Any
Функция: установка условий для PCP. Когда значение PCP в пакете, полученном портом-участником, соответствует настройкам этого параметра, условие выполняется успешно. Этот параметр недоступен, если для параметра «Tag» установлено значение «Untagged».

DEI
Опции: Any/0/1
Значение по умолчанию: Any
Функция: установка условий для DEI. Когда значение DEI в пакете, полученном портом-участником, соответствует настройкам этого параметра, условие выполняется успешно. Этот параметр недоступен, если для параметра «Tag» установлено значение «Untagged».
Frame Type
Опции: Any/EtherType/LLC/SNAP/IPv4/IPv6
Значение по умолчанию: Any
Функция: выбор типа кадра.

10.3. Настройка параметров EtherType.

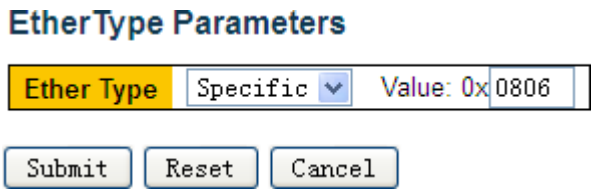


Рис. 74. Настройка параметров EtherType

Ether Type
Опции: Any/Specific (0x0600 ~ 0xFFFF)
Значение по умолчанию: Any
Функция: установка условий для DEI. Если установлено значение «Specific», необходимо указать тип Ethernet. Когда пакет Ethernet, полученный портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.
10.4. Настройка параметров кадра LLC.

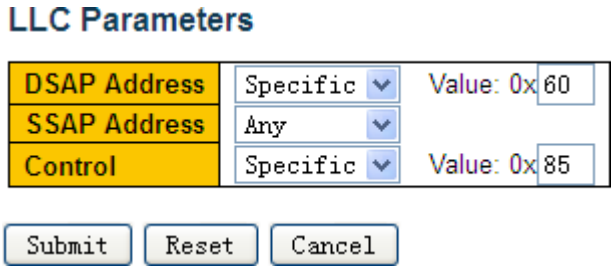


Рис. 75. Настройка параметров кадра LLC

DSAP Address/SSAP Address/Control
Опции: Any/Specific (0x00 ~ 0xFF)
Значение по умолчанию: Any
Функция: установка условий для параметров пакета LLC. Если для параметров «DSAP Address», «SSAP Address» или «Control» задано значение «Specific», необходимо ввести конкретное значение. Когда пакет LLC, полученный портом-участником, соответствует настройкам этих параметров, условие выполняется успешно.

10.5. Настройка параметров кадра SNAP.

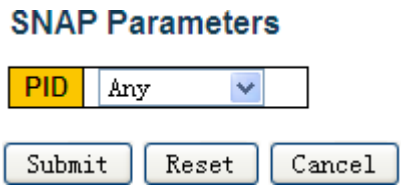


Рис. 76. Настройка параметров кадра SNAP

PID
Опции: Any/Specific (0x0000 ~ 0xFFFF)
Значение по умолчанию: Any
Функция: установка условий для параметров пакета SNAP. Если установлено значение «Specific», необходимо ввести значение PID. Когда PID в пакете SNAP, полученном портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.

10.6. Настройка параметров кадра IPv4/ IPv6.

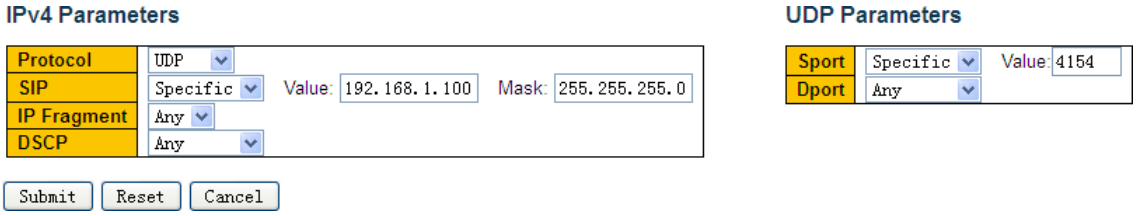


Рис. 77. Настройка параметров кадра IPv4

Protocol
Опции: Any/UDP/TCP/Other (0 ~ 255)
Значение по умолчанию: Any
Функция: установка условий для типа протокола пакета IPv4. Если установлено значение UDP или TCP, необходимо установить идентификатор порта источника и идентификатор порта назначения. Если установлено значение «Other», необходимо установить идентификатор протокола. Когда тип протокола в пакете, полученном портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.
Sport/ Dport
Опции: Any/Specific (0 ~ 65535)/Range (0 ~ 65535)
Значение по умолчанию: Any
Функция: установка условий для идентификатора (ID) порта источника и ID порта назначения. Если для них установлено значение «Specific», необходимо указать идентификатор порта. Если для них установлено значение «Range», необходимо указать диапазон идентификаторов портов. Когда идентификаторы портов в IP-пакете, полученные портом-участником, соответствуют настройкам этого параметра, условие выполняется успешно.
SIP
Опции: Any/Specific

Значение по умолчанию: Any
Функция: установка условий для IP-адреса источника и маски IP-адреса источника. Если для него установлено значение «Specific», необходимо назначить IP-адрес и маску IP-адреса. Когда SIP в IP-пакете, полученным портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.

IP Fragment

Опции: Any/Yes/No
Значение по умолчанию: Any
Функция: установка условий для пакета IP-фрагмента. Если фрагмент (fragment) в пакете IPv4, полученным портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.

DSCP

Опции: Any/Specific (0 ~ 63)/Range (0 ~ 63)
Значение по умолчанию: Any
Функция: установка условий для значения DSCP. Если установлено значение «Specific», необходимо ввести значение DSCP. Если установлено значение «Range», необходимо установить диапазон DSCP. Когда DSCP в IP-пакете, полученным портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.

10.7. Настройка параметров действий QCL.

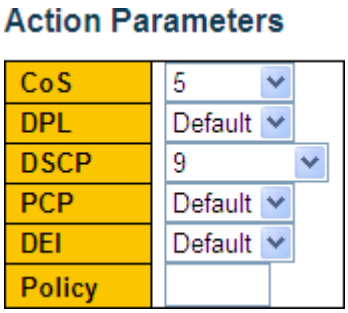


Рис. 78. Настройка параметров действий QCL

CoS

Опции: 0 ~ 7/Default
Значение по умолчанию: 0
Функция: значение CoS определяет очередь для хранения пакетов. Значение CoS находится в диапазоне от 0 до 7, что соответствует очереди от 0 до 7. Значение «Default» означает, что значение CoS равно 0. Когда пакет, полученный портом-участником, совпадает с записью QCL, коммутатор выделяет значение CoS для пакет.

DPL

Опции: Default/0/1
Значение по умолчанию: Default
Функция: изменение значения DPL в пакете, полученным портом-участником, на значение этого параметра, если пакет содержит запись QCL. Значение «Default» указывает, что значение DPL в пакете не изменилось.

DSCP
Опции: Default/0 ~ 63
Значение по умолчанию: Default
Функция: изменение значения DSCP в пакете, полученным портом-участником, на значение этого параметра, если пакет содержит запись QCL. Значение «Default» указывает, что значение DSCP в пакете не изменилось.
PCP
Опции: Default/0 ~ 7
Значение по умолчанию: Default
Функция: изменение значения PCP в пакете, полученным портом-участником, на значение этого параметра, если пакет содержит запись QCL. Значение «Default» указывает, что значение DSCP в пакете не изменилось.
DEI
Опции: Default/0/1
Значение по умолчанию: Default
Функция: изменение значения DEI в пакете, полученным портом-участником, на значение этого параметра, если пакет содержит запись QCL. Значение «Default» указывает, что значение DSCP в пакете не изменилось.

Значение PCP и значение DEI в пакете не могут быть изменены отдельно. То есть значения PCP и DEI должны быть изменены одновременно или сохранить свои исходные значения.

10.8. Просмотр записей QCL.

QoS Control List Status

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
Static	1	2	Any	5	Default	Default	Default	Default	Default	No
Static	2	3	Any	6	Default	Default	6	0	Default	No
Static	3	4	IPv4	7	1	9	Default	Default	Default	No
Static	5	Any	Any	1	Default	Default	Default	Default	Default	No
Static	4	Any	Any	2	Default	Default	Default	Default	Default	No

Рис. 79. Просмотр записей QCL

Conflict
Опции: No/Yes (Нет/Да).
Функция: отображает статус конфликтов записей QCL. Если ресурсов для создания записи QCL недостаточно, значение поля «Conflict» устанавливается в «Yes» для этой записи. В противном случае для этой записи устанавливается значение «No».
Нажмите <Resolve Confilct>, чтобы освободить ресурсы, необходимые для конфликтующих записей QCL.

11. Настройка ограничений для входящего порта.

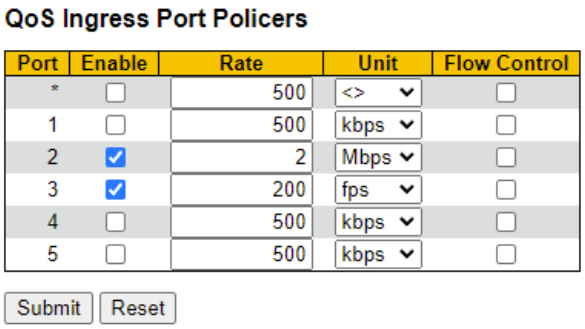


Рис. 80. Настройка ограничений входящего порта

Enable
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: включение и выключение ограничений для входящего порта. Контроль трафика порта реализуется с помощью ограничения скорости порта или функции управления потоком.
Rate, Unit
Настраиваемый диапазон: 100 ~ 3276700 Кбит/с / 1 ~ 3276 Мбит/с / 100 ~ 3276700 Кдр/с / 1 ~ 3276 Ккдр/с
Значение по умолчанию: 500 Кбит/с
Функция: ограничение скорости пакетов, получаемых портом. Пакеты со скоростью, превышающей значение, отбрасываются.
Flow Control
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: включение и выключение функции управления потоком для порта. После включения этой функции в случае, когда трафик, полученный портом, превышает предельное значение, отправитель с помощью алгоритмов или протоколов получает указание замедлить передачу, чтобы предотвратить потерю пакетов.

Предварительным условием для того, чтобы функция управления потоком вступила в силу, является включение управления потоком порта на странице конфигурации порта.

12. Настройка ограничений для входящих очередей.

QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2			Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable
*	☐	☐	☐	500	<>	☐	☐	☐	☐	☐
1	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
2	☐	☐	☑	20	Mbps	☐	☐	☐	☐	☐
3	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
4	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
5	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐

Submit Reset

Рис. 81. Настройка ограничений для входящих очередей

E
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: включение или выключение ограничений для входящих очередей. Необходимо установить параметры скорости после включения контроля трафика для очередей.
Rate, Unit
Настраиваемый диапазон: 100 ~ 3276700 Кбит/с / 1 ~ 3276 Мбит/с
Значение по умолчанию: 500 Кбит/с
Функция: ограничение скорости пакетов, получаемых очередями. Пакеты со скоростью, превышающей значение, отбрасываются.

13. Настройка режима планирования для очередей.

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-

Рис. 82. Просмотр режима планирования для очередей

Нажмите <Port>, чтобы войти на страницу конфигурации «режима планирования очереди портов».

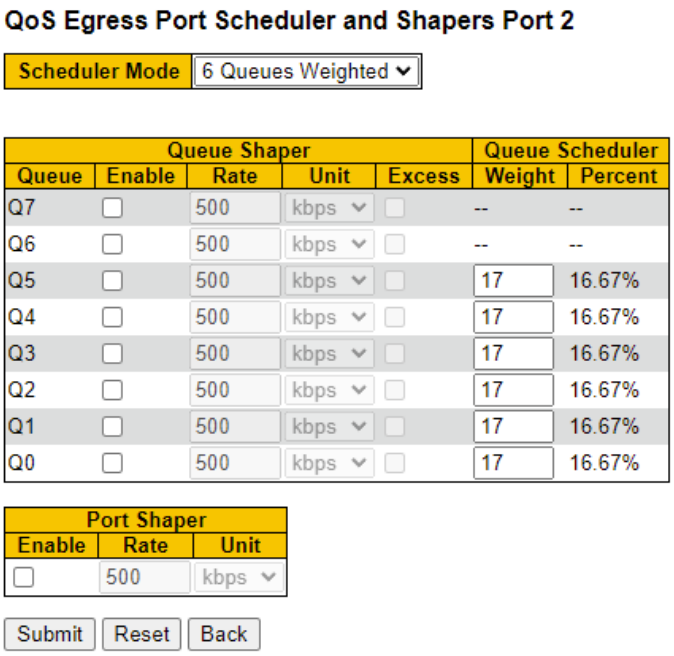


Рис. 83. Режим планирования очереди портов

Scheduler Mode
Опции: Strict Priority/6 Queues Weighted (Строгий приоритет/6 взвешенных очередей)
Значение по умолчанию: Strict Priority (Строгий приоритет)
Функция: настройка режима исходящей очереди для выбранного порта.
Взвешенная очередь (Queue Weight)
Настраиваемый диапазон: 1 ~ 100
Значение по умолчанию: 17
Функция: настройка весовых значений очереди.
Вы можете выбрать порт для настройки режима планирования очереди в правом верхнем углу страницы.

14. Настройка формирования трафика исходящего порта.

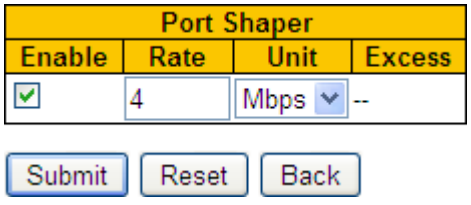


Рис. 84. Настройка формирования трафика исходящего порта

Enable
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: включение и выключение формирования трафика для исходящего порта. Формирование трафика порта реализуется ограничением скорости порта.

Rate, Unit
Настраиваемый диапазон: 100 ~ 3281943 Кбит/с / 1 ~ 3281 Мбит/с
Значение по умолчанию: 500 Кбит/с
Функция: ограничение скорости пакетов, передаваемых портом. Пакеты со скоростью, превышающей значение, отбрасываются.
Нажмите <Back>, чтобы закрыть текущую страницу конфигурации и вернуться к предыдущей странице.
Вы можете выбрать порт для настройки формирования трафика в правом верхнем углу страницы.

15. Настройка формирования очередей.

Queue Shaper					Queue Scheduler	
Queue	Enable	Rate	Unit	Excess	Weight	Percent
Q7	☐	500	kbps	☐	--	--
Q6	☑	4	Mbps	☐	--	--
Q5	☑	8	Mbps	☑	20	13%
Q4	☐	500	kbps	☐	20	13%
Q3	☐	500	kbps	☐	20	13%
Q2	☐	500	kbps	☐	40	25%
Q1	☐	500	kbps	☐	40	25%
Q0	☐	500	kbps	☐	20	13%

Рис. 85. Настройка формирования очередей

Enable
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: включение и выключение режима формирования очередей.
Rate, Unit
Настраиваемый диапазон: 100~3281943 Кбит/с / 1~3281 Мбит/с
Значение по умолчанию: 500 Кбит/с
Функция: ограничение скорости пакетов, передаваемых очередью. Пакеты со скоростью, превышающей значение, отбрасываются.
Нажмите <Back>, чтобы закрыть текущую страницу конфигурации и вернуться к предыдущей странице.
Вы можете выбрать порт для настройки формирования трафика в правом верхнем углу страницы.

16. Настройка управления штормами на порту.

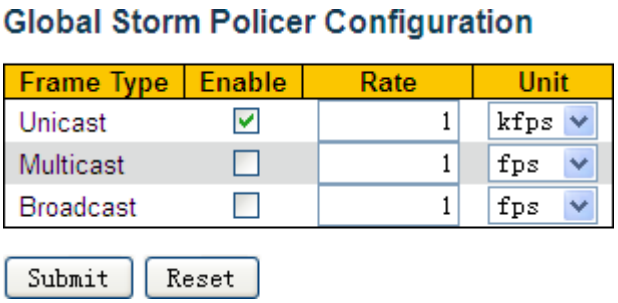


Рис. 86. Управление штормами

Режим управления штормами предназначен для ограничения принимаемых портом broadcast/unknown multicast/unknown (широковещательных/неизвестных многоадресных /неизвестных одноадресных пакетов). Когда скорость данных пакетов, полученных через порт, превышает настроенный порог, система отбрасывает пакеты, чтобы сохранить трафик в допустимом диапазоне для обеспечения нормальной работы сети.

Enable

Опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Функция: включение и выключение режима управления штормами.

Rate, Unit

Настраиваемый диапазон: 1~1024000 Кдр/с / 1~1024 Ккдр/с

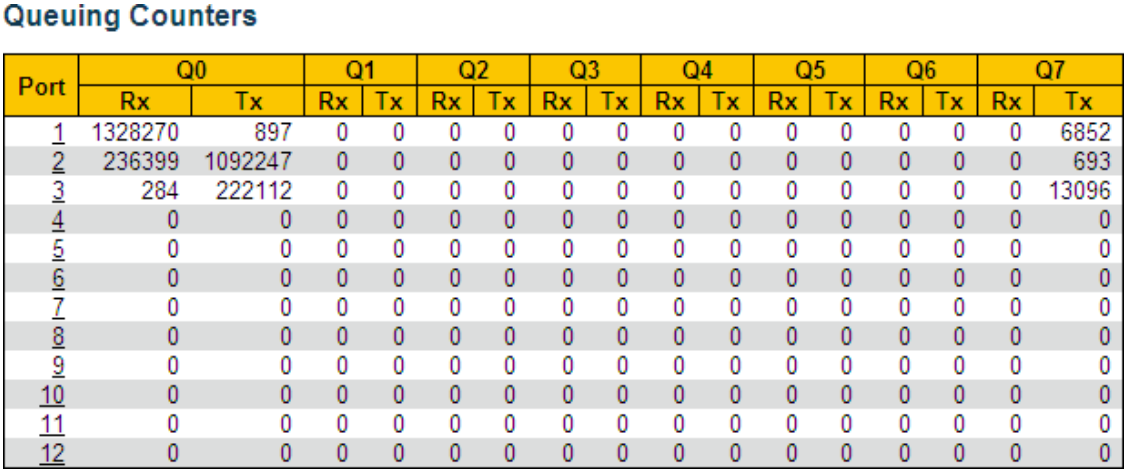
Значение по умолчанию: 1 Кдр/с

Функция: настройка порога для ограничения пропускной способности порта. Пакеты, превышающие порог, будут отброшены.

Нажмите <Back>, чтобы закрыть текущую страницу конфигурации и вернуться к предыдущей странице.

Вы можете выбрать порт для настройки формирования трафика в правом верхнем углу страницы.

17. Просмотр счетчиков очереди.



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	1328270	897	0	0	0	0	0	0	0	0	0	0	0	0	0	6852
2	236399	1092247	0	0	0	0	0	0	0	0	0	0	0	0	0	693
3	284	222112	0	0	0	0	0	0	0	0	0	0	0	0	0	13096
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Рис. 87. Просмотр счетчиков очереди

Отображение количества пакетов, которые отправляет/получает каждая очередь.
Нажмите <port>, чтобы перейти на страницу отображения подробной статистики порта (см. рис. 59).

8.4. Пример типовой настройки

Как показано на рис. 92, порты 1-5 пересылают сообщения в порт 6. Пакеты, принимаемые портом 1, являются не тегированными и соответствуют очереди 2.
Значение PCP пакетов, принимаемых портом 2, равно «0», значение DEI равно «1». Пакеты, принимаемые портом 2, соответствуют очереди 3.
Значение DSCP пакетов, принимаемых портом 3, равно «4». Пакеты, принимаемые портом 3, соответствуют очереди 6.
Порт 4 сопоставляет все полученные пакеты от источника с MAC-адресом 00-00-00-00-00-23 с очередью 5 и для последующей пересылки заменяет значение DSCP в этих пакетах на «9».
Значение DSCP пакетов, принимаемых портом 5, равно «5». Пакеты, принимаемые портом 5, соответствуют очереди 2.
Шаги настройки коммутатора:

1. Настройте значение CoS порта 1 равным «2» (см рис. 60).
2. Включите режим классификации тега порта 2 и сопоставьте (PCP=0, DEI=1) с CoS=3 (см. рис. 61).
3. Включите сопоставление на основе DSCP портов 3 и 5 (см. рис. 66).
4. Установите значения «4» и «5» DSCP как «Доверенные» и сопоставьте значение «4» DSCP с очередью 6, а значение «5» DSCP с очередью 2 (см. рис 68).
5. Включите записи QCL для порта 4 (см. рис. 72).
6. Настройте параметры записей QCL: установите значение SMSC как 00-00-00-00-00-23, а тип кадра как IPv4 (см. рис. 75).
7. Настройте параметры действия записей QCL: установите значение CoS как «5», а значение DSCP как «9» (см. рис. 78).
8. Настройте режим планирования очереди порта 6 на 6 взвешенных очередей, вес очереди от Q0 ~ Q5 как 20, 40, 40, 20, 20, 20 (см. рис. 83).

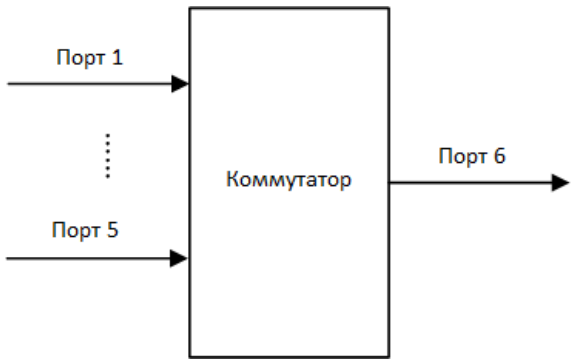


Рис. 88. Пример настройки QoS

Пакеты портов 1 и 5 входят в очередь 2, пакеты порта 2 входят в очередь 3, пакеты порта 3 входят в очередь 6, пакеты порта 4 входят в очередь 5.

Очередь 6 и очередь 7 используют режим планирования со строгим приоритетом (Strict priority), а очереди с 0 по 5 используют режим планирования WRR. Данные в очереди 6 обрабатываются первыми. Когда очередь 6 пуста, данные в очередях с 0 по 5 планируются по весовому соотношению.
Вес очереди - 20, 40, 40, 20, 20, 20. Таким образом, доля полосы пропускания, выделенная пакетам входящей очереди 2, составляет 40 / (20 + 40 + 40 + 20 + 20 + 20) = 25%, пакетам входящей очереди 3: 20 / (20 + 40 + 40 + 20 + 20 + 20) = 13%, а пакетам входящей очереди 5: 20 / (20 + 40 + 40 + 20 + 20 + 20) = 13%. Пакеты портов 1 и 5 входят в очередь 2, поэтому они пересылаются в соответствии с правилом FIFO (First In, First out «первым пришел - первым ушел), однако общая доля пропускной способности портов 1 и 5 должна составлять 25%.

9. Безопасность (Security)

9.1. Управление пользователями

9.1.1. Введение

Во избежание проблем с безопасностью, вызванных подключением незаконных пользователей, коммутаторы данной серии обеспечивают иерархическое управление пользователями. Коммутатор предоставляет различные права по подключению в зависимости от уровня пользователя. Доступны три уровня пользователя:
Табл. 5

Уровень пользователя	**Привилегированный режим**	**Описание**
Guest	5 ~ 9	Самый низкий уровень, который позволяет только просматривать конфигурацию коммутатора
System	10 ~ 14	Средний уровень, пользователи системы имеют определенные права доступа и настройки. Пользователи системы не могут получить доступ к следующим функциям: управление пользователями, обновление программного обеспечения, перезагрузка, загрузка по умолчанию и передача файлов.
Admin	15	Самый высокий уровень, администраторы имеют права на выполнение всех функций.

9.1.2. Настройка через WEB-интерфейс

1. Сознание новых пользователей.

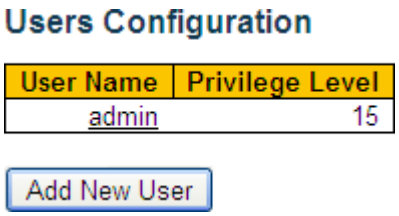


Рис. 89. Создание новых пользователей

Нажмите <Add New User>, чтобы добавить нового пользователя. Коммутатор поддерживает максимум 20 пользователей.

2. Настройка уровня доступа пользователей.

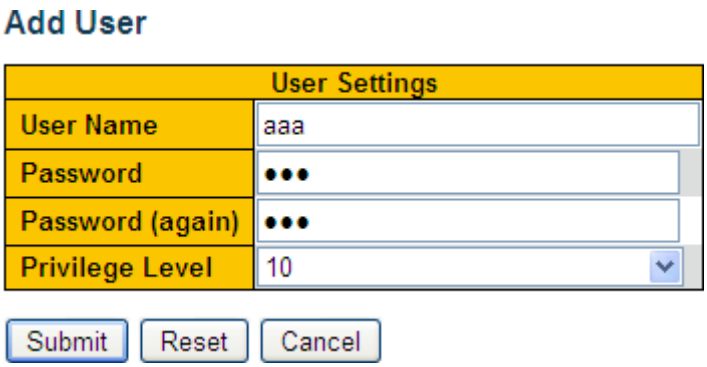


Рис. 90. Настройка уровня доступа пользователей

Имя пользователя (User Name)
Настраиваемый диапазон: 1~31 символов.
Функция: настройка имени пользователя.
Пароль (Password)
Настраиваемый диапазон: 1~31 символов.
Функция: настройка пароля, который будет использовать пользователь для подключения к коммутатору.
Подтверждение пароля (Password (again))
Настраиваемый диапазон: 1~31 символов.
Функция: подтверждение пароля доступа.
Уровень доступа (Privilege Level)
Настраиваемый диапазон: 1~15.
Функция: настройка уровня пользователя. Разные уровни доступа пользователей имеют разные права доступа.

3. Просмотр списка пользователей.

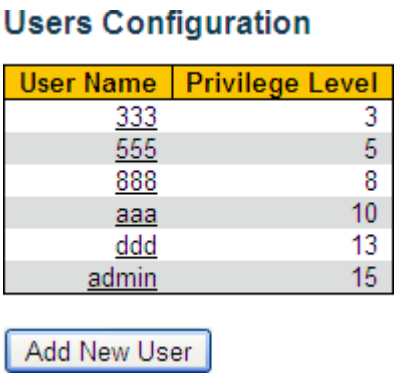


Рис. 91. Список пользователей

Нажмите <User Name>, чтобы изменить текущие настройки пользователя.

4. Изменение настроек пользователя.

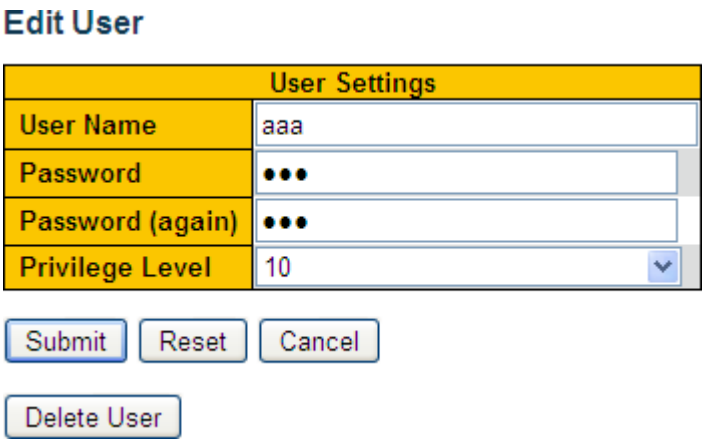


Рис. 92. Список пользователей

Вы можете изменить пароль пользователя и его уровень доступа.
Нажмите <Delete User> для удаления пользователя.

- Пользователь «Admin» не может быть удален.
- Уровень привилегий для пользователя «Admin» по умолчанию: 15 и не может быть изменен. Можно изменить только пароль пользователя «Admin».

5. Настройка уровня привилегий для групп пользователей.

Privilege Level Configuration

Group Name	Privilege Level			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
ALARM	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
ETHERNETIP	5	10	5	10
GMRP	5	10	5	10
IP	5	10	5	10
IPC	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LINKCHECK	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
MODBUS	5	10	5	10
Operate_Log	5	10	5	10
PNIO_DEV	5	10	5	10
Ports	5	10	1	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security	5	10	5	10
SNTP	5	10	5	10
Spanning_Tree	5	10	5	10
Sy2-Ring	5	10	5	10
Sy2-RP	5	10	5	10
System	5	10	1	10
VLANs	5	10	5	10

Submit Reset

Рис. 93. Уровень привилегий для групп пользователей

Когда уровень привилегий пользователя такой же или выше, чем уровень привилегий группы, пользователь может получить доступ к группе или настроить ее. Право доступа или настройки зависит от уровня привилегий пользователя.

9.2. Настройка аутентификации

1. Настройка режима доступа к коммутатору, режима и порядка аутентификации.

Authentication Method Configuration

Client	Method		
console	no	no	no
telnet	tacacs	local	no
ssh	radius	tacacs	local
http	local	no	no

Рис. 94. Настройка режима аутентификации

Режим доступа (Client)

Опции: console/telnet/ssh/http.

Функция: выбор режима доступа к коммутатору.

Метод 1/Метод 2/Метод 3 (Method 1/Method 2/Method 3)
Опции: no/local/tacacs/radius.
Значение по умолчанию: local
Функция: методы в таблице показаны слева направо: Метод 1, Метод 2 и Метод 3. Сначала выполняется метод аутентификации 1. Если аутентификация не удалась, применяется метод аутентификации 2. Если и метод аутентификации 1, и метод аутентификации 2 неудачны, выполняется метод аутентификации 3.
Описание: «no» означает, что аутентификация отключена и вход в систему невозможен; «local» подразумевает, что для выполнения аутентификации используются имя пользователя и пароль, установленные на локальном уровне; «tacacs» означает использование имени пользователя и пароля, установленных на сервере TACACS +; «radius» означает использование имени пользователя и пароля, установленных на сервере RADIUS для аутентификации.

Если для метода 1 и метода 2 выбраны режимы «tacacs/radius», рекомендуется настроить метод 3 как «local». Это позволит выполнить вход в систему для локального пользователя, если ни один из настроенных удаленных серверов аутентификации не работает.

9.3. Настройка протокола SSH

9.3.1. Введение

SSH - это сетевой протокол для безопасного удаленного входа в систему. Он шифрует все передаваемые данные, чтобы предотвратить раскрытие информации. Когда данные шифруются с помощью SSH, пользователи могут использовать только режим командной строки для настройки коммутаторов.
Данная серия коммутаторов поддерживает функцию сервера SSH и дает возможность подключаться множеству клиентов SSH, которые могут подключиться к удаленному коммутатору посредством протокола SSH.

9.3.2. Реализация

Чтобы осуществить безопасное SSH подключение, сервер и клиент должны пройти следующие пять этапов:

- Стадия согласования версий: в настоящее время SSH состоит из двух версий: SSH1 и SSH2. Обе стороны должны согласовать версию для использования;
- Стадия согласования ключей и алгоритмов: SSH поддерживает несколько типов алгоритмов шифрования. Обе стороны должны согласовать, какой алгоритм будет использоваться;
- Стадия аутентификации: клиент SSH отправляет на сервер запрос на аутентификацию, после чего сервер должен аутентифицировать клиента;
- Стадия запроса сеанса: клиент отправляет запрос на сеанс к серверу после прохождения аутентификации;
- Стадия сессии: клиент и сервер начинают связь после передачи запроса на сеанс.

1. Включение протокола SSH.

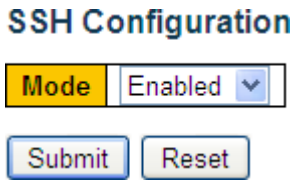


Рис. 95. Включение протокола SSH

Режим (Mode)
Опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Enable (Включено)
Функция: включение и выключение протокола SSH. Если режим работы протокола включен, коммутатор работает ка сервер SSH.

9.3.3. Пример типовой настройки

Хост работает как клиент SSH для установления локального соединения с коммутатором, как показано на рисунке 102.

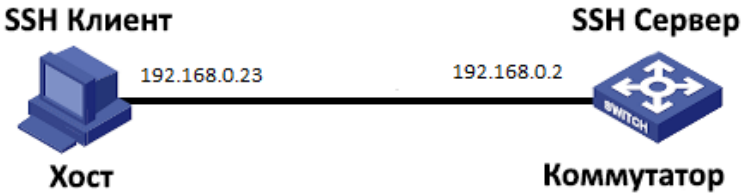


Рис. 96. Включение протокола SSH

1. Включите протокол SSH.
2. Установите соединение с SSH-сервером. Сначала запустите программу PuTTY.exe, как показано на рис. 97; введите IP-адрес SSH-сервера «192. 168.0.2» в поле имени хоста (или IP-адреса).

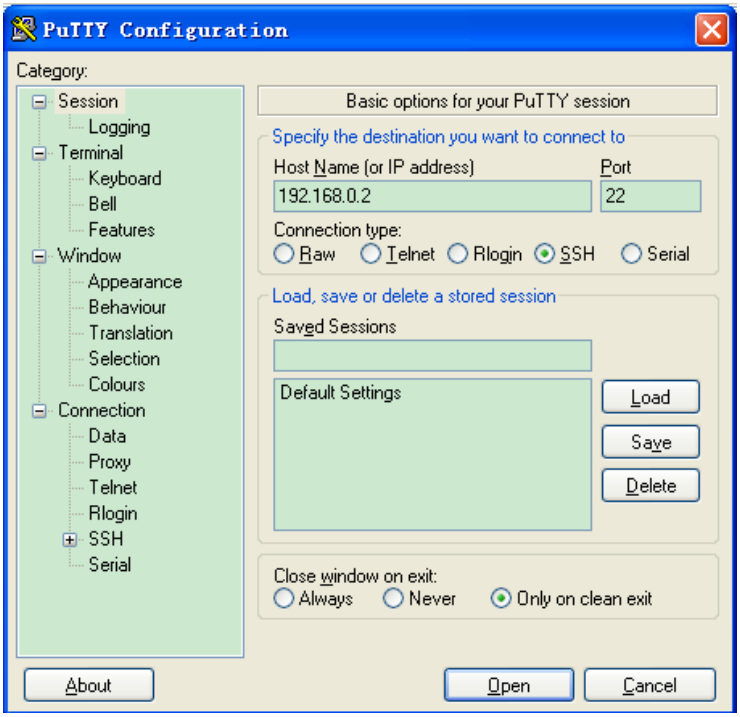


Рис. 97. Включение протокола SSH

3. Нажмите кнопку <Open>, после этого появится предупреждающее сообщение, показанное на рис. 98. Нажмите кнопку <Да>.

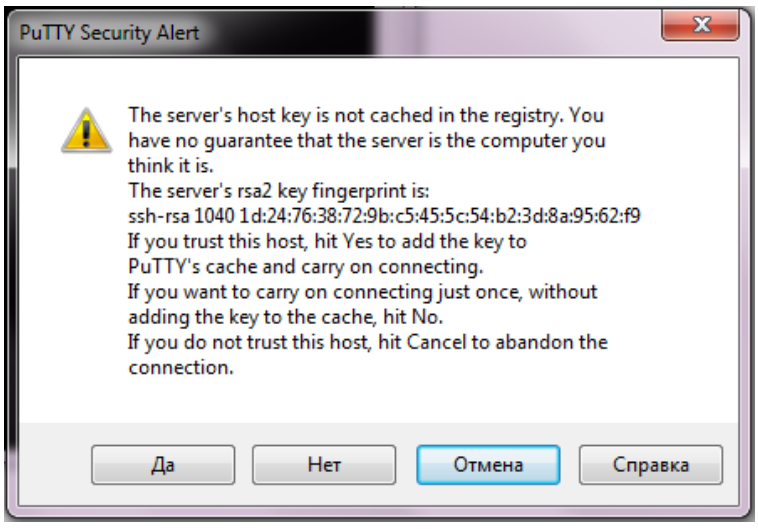


Рис. 98. Предупреждающее сообщение

4. Введите имя клиента «admin» и пароль «123», для того чтобы войти в интерфейс настроек коммутатора (рис. 99).

Рис. 99. Интерфейс авторизации

9.4. Настройка протокола SSL

9.4.1. Введение

SSL (Secure Socket Layer) - это протокол безопасности, который обеспечивает безопасную связь на уровне протоколов приложения TCP, например, HTTPS. SSL шифрует сетевое соединение на транспортном уровне и использует симметричный алгоритм шифрования для обеспечения безопасности данных. Протокол SSL использует код аутентификации на базе секретного ключа для сохранения передаваемой и принимаемой информации. Этот протокол широко применяется в веб-браузерах, электронной почте, и т.д., используя протоколы шифрования для безопасной передачи информации по сети.
Для доступа к коммутатору с включенным протоколом SSL, пользователи должны использовать безопасное подключение с использованием https, например https://192.168.0.2.

9.4.2. Настройка через WEB-интерфейс

1. Включение протокола HTTPS.

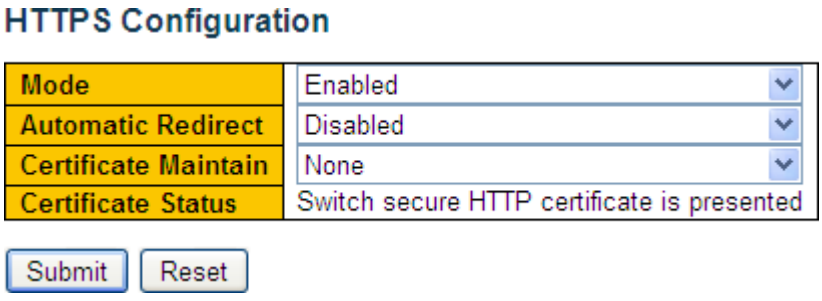


Рис. 100. Включение протокола HTTPS

Режим (Mode)

Опции: Enable/Disable (Включено/Выключено)

Значение по умолчанию: Enable (Включено)

Функция: включение и отключение протокола HTTPS. После включения HTTPS пользователи для доступа к коммутатору могут использовать ссылку http://ip-address и защищенную ссылку https://ip- address.

Автоматическое перенаправление (Automatic Redirect)

Опции: Enable/Disable (Включено/Выключено)

Значение по умолчанию: Enable (Включено)

Функция: Enable (Включено) означает, что пользователи должны использовать только защищенную ссылку https://ip-address для доступа к коммутатору. Disable (Выключено) означает, что пользователи могут использовать как ссылку http://ip-address, таки и защищенную ссылку https://ip-address для доступа к коммутатору. Параметр «Автоматическое перенаправление» можно настроить, только если включен режим HTTPS.

Управление сертификатом (Certificate Maintain)

Опции: Enable/Disable (Включено/Выключено)

Значение по умолчанию: Enable (Включено)

Функция: управление сертификатом HTTPS. Параметр «Certificate Maintain» можно настроить, только если отключен режим HTTPS. «Delete» (удалить) используется для удаления существующего сертификата HTTPS из коммутатора. «Upload» (загрузка) используется для загрузки правильного сертификата HTTPS на коммутатор с помощью веб-браузера или URL-адреса. «Generate» (генерация) указывает, что коммутатор автоматически генерирует правильный сертификат HTTPS.

Статус сертификата (Certificate Status)

Опции: Switch secure HTTP certificate is presented/Switch secure HTTP certificate is not presented/Switch secure HTTP certificate is generating (Сертификат представлен/Сертификат не представлен/Сертификат создается).

Функция: отображение статуса сертификата HTTPS для коммутатора. «Сертификат представлен» означает, что сертификат доступен. В этом случае вы можете войти на веб-страницу коммутатора через HTTPS. «Сертификат не представлен» означает, что на коммутаторе нет доступных сертификатов. В этом случае вы не можете войти на веб-страницу через HTTPS. Создание сертификата безопасности коммутатора HTTP означает, что создается сертификат HTTPS.

2. Генерация сертификата HTTPS.

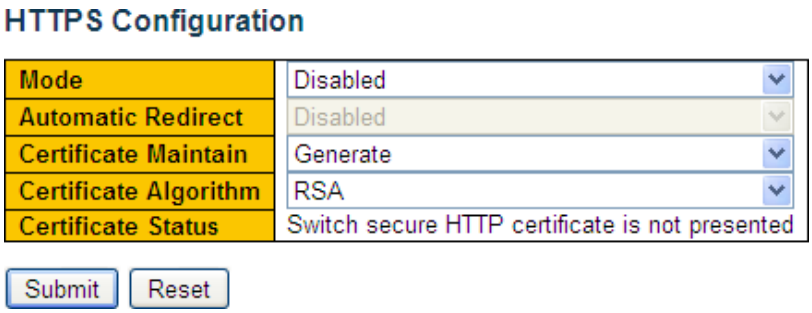


Рис. 101. Генерация сертификата

Статус сертификата (Certificate Status)
Опции: RSA/DSA.
Значение по умолчанию: RSA.
Функция: выбор алгоритма для выбора сертификата HTTPS.

3. Загрузка сертификата HTTPS.

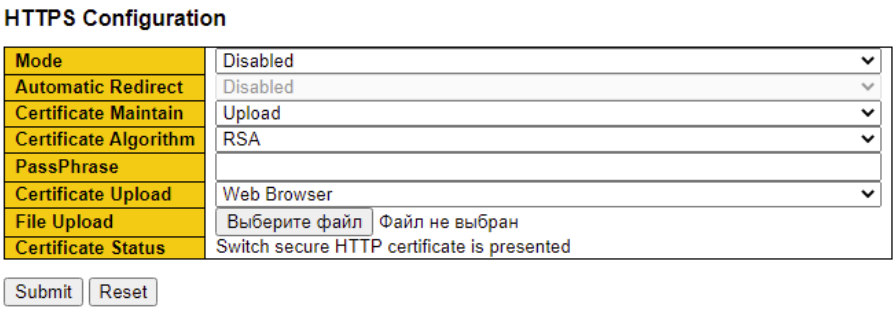


Рис. 102. Загрузка сертификата через веб-браузер

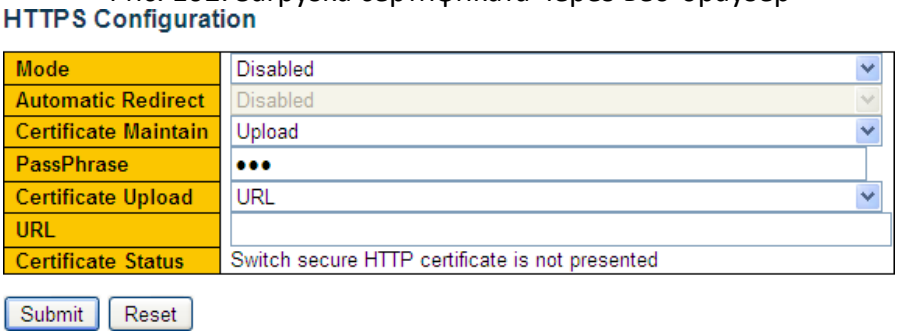


Рис. 103. Загрузка сертификата через URL

Пароль (PassPhrase)
Функция: используется для шифрования сертификата.

Загрузка сертификата (Certificate Upload)
Опции: Web Browser/URL.
Значение по умолчанию: Web Browser.
Функция: выбор метода для загрузки сертификата HTTPS.
Загрузка файла (File Upload)
Функция: выбор файла с сертификатом HTTPS записанного на локальном сервере.
URL
Функция: настройка пути хранения файла сертификата HTTPS. Поддерживаемые протоколы: HTTP, HTTPS, TFTP и FTP. Формат настройки следующий:
http://10.10.10.10:80/new_image_path/new_image.dat или
FTP://username:password@10.10.10.10/new_image_path/new_image.dat.

4. Если сертификат HTTPS представлен в коммутаторе, введите имя пользователя и пароль для успешного входа в коммутатор через HTTPS.

9.5. Управление доступом

9.5.1. Введение

Для управления доступом к коммутатору можно создать список доступа для того, чтобы ограничить количество хостов, которые могут получить доступ к коммутатору. Список доступа может содержать до 16 записей. Хост, который соответствует любой из записей в списке доступа, может успешно получить доступ к коммутатору.

1. Настройка списка доступа

Нажмите <Add New Entry>, чтобы настроить список управления доступом. Коммутатор поддерживает список управления доступом максимум из 16 записей.

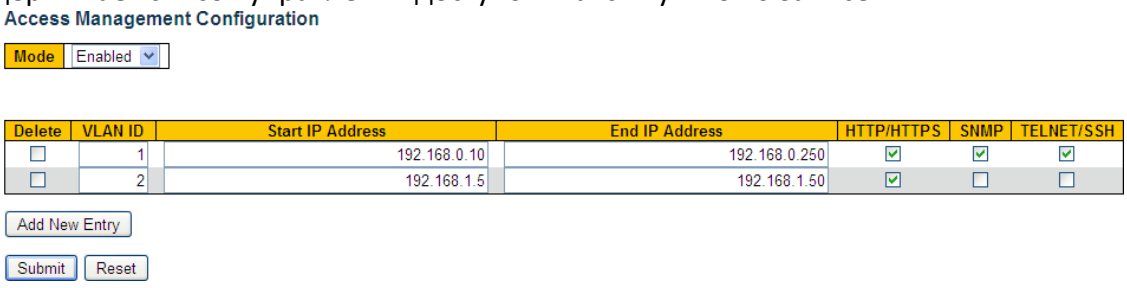


Рис. 104. Настройка списка доступа

Режим (Mode)
Опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Disable (Выключено)
Функция: включение и выключение режима управления доступом к коммутатору. Disable (Выключено): доступ к коммутатору не ограничен.
Идентификатор VLAN (VLAN ID)
Настраиваемый диапазон: 1 ~ 4094

Функция: настройка идентификатора VLAN для списка управления доступом.

Начальный IP-адрес/Конечный IP-адрес (Start IP Address/End IP Address)

Функция: настройка диапазона IP-адресов для списка управления доступом.

HTTP/HTTPS

Функция: если выбран режим HTTP/HTTPS, хост, который соответствует идентификатору VLAN и IP-адресу в списке доступа, может получить доступ к коммутатору через HTTP/HTTPS.

SNMP

Функция: если выбран режим SNMP, хост, который соответствует идентификатору VLAN и IP-адресу в списке доступа, может получить доступ к коммутатору через SNMP.

TELNET/SSH

Функция: если выбран TELNET/SSH, хост, который соответствует идентификатору VLAN и IP-адресу в списке доступа, может получить доступ к коммутатору через TELNET/SSH.

2. Просмотр статистики управления доступом.

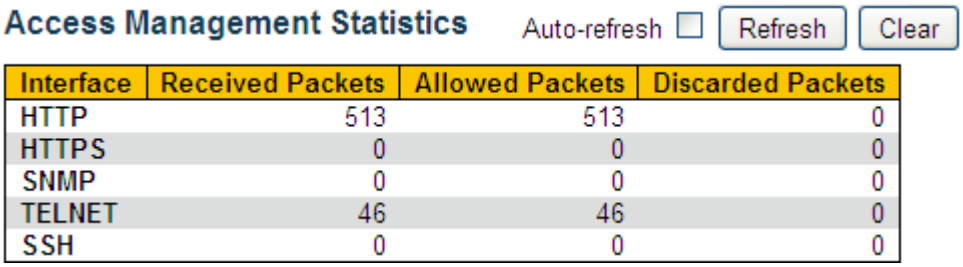


Рис. 105. Просмотр статистики управления доступом

3. Настройка таймаутов для режимов доступа к коммутатору.

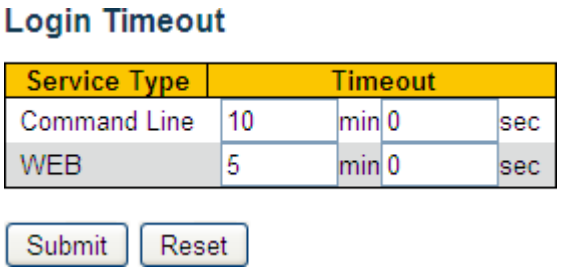


Рис. 106. Настройка таймаутов

Режим (Mode)

Настаиваемый диапазон: (0~1440) мин. (0~3600) сек.

Значение по умолчанию: 10 мин. для CLI, 5 мин. для web-интерфейса.

Функция: настройка времени ожидания входа пользователя и времени его отключения. Отсчет времени начинается, когда пользователь завершит все настройки. Система автоматически отключит режим доступа, когда время закончится. Если время установлено

на 0, функция тайм-аута отключена. В этом случае сервер не будет проверять, истекло ли время работы пользователя в системе, и, следовательно, пользователь не будет отключен от системы.

9.6. Протокол SNMP v1/SNMP v2c

9.6.1. Введение

Simple Network Management Protocol (SNMP) - протокол управления сетевыми устройствами с использованием протокола TCP/IP. Благодаря функции SNMP, администратор может запрашивать информацию об устройстве, менять настройки, следить за состоянием устройства и обнаруживать неполадки сети.

9.6.2. Реализация

Для управления устройствами, SNMP использует архитектуру «manager/agent» (менеджер/агент). Таким образом, по функциональности он включает две составляющие: «NMS» и «Агент».

- Network Management Station (NMS) - это рабочая станция, на которой работает SNMP-приложение для управления сетью клиентов, играющая основную роль в управлении сетью с помощью протокола SNMP.
- Агент - это программный процесс на управляемом устройстве. Он отвечает за прием и обработку запросов от NMS. При возникновении аварийной ситуации агент автоматически информирует об этом NMS.

NMS является средством управления сетью SNMP, а Агент управляется сетью SNMP. Обмен информацией управления между NMS и Агентом осуществляется через протокол SNMP. SNMP обеспечивает выполнение 5 основных операций:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

NMS отправляет пакеты «Get-Request», «Get-Next-Request» и «Set-Request» для запроса данных, настройки и управления устройством. После получения этих запросов, Агенты отвечают пакетами «Get-Response». При возникновении тревоги агент автоматически отправит сообщение «Trap» в NMS, чтобы сообщить о возникновении аномальных событий.

9.6.3. Описание

Данная серия коммутаторов поддерживает версии SNMPv2c и SNMPv3. При этом SNMPv2 совместим с SNMPv1.

SNMPv1 использует принцип аутентификации по имени сообщества (Community Name Authentication). Имя сообщества работает как пароль и используется для ограничения доступа Агента SNMP к SNMP NMS. Если имя сообщества SNMP-сообщения не может пройти аутентификацию устройства, отправленное сообщение будет удалено.

SNMPv2 также использует аутентификацию по имени сообщества. Он не просто совместим с SNMPv1, но и расширяет функции SNMPv1. Корректная совместная работа NMS и Агента основывается на согласованной версии SNMP. Агент может быть настроен для работы с несколькими версиями одновременно и использовать разные версии для связи с разными NMS.

9.6.4. Описание MIB (Management Information Base)

Любой управляемый ресурс можно рассматривать как объект, соответственно он называется управляемым объектом.

MIB (Management Information Base) - это совокупность всех управляемых объектов. MIB определяет иерархические отношения между управляемыми объектами и определяет основные атрибуты объектов, например, имя объекта, права доступа, типы данных и т.д. У каждого Агента есть своя MIB. NMS может читать или записывать объекты в MIB в соответствии со своими правами. Связь NMS, Агента и MIB показана (см рис. 107).

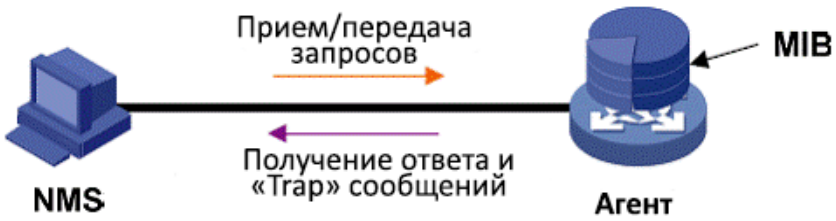


Рис. 107. Взаимосвязь NMS, Агента и базы MIB

MIB определяет древовидную структуру, где каждый узел дерева является управляемым объектом. Каждый узел дерева содержит OID (Идентификатор объекта), который может указывать позицию узла в структуре дерева MIB. OID управляемого объекта A равен 1.2.1.1 (см. рис. 108).

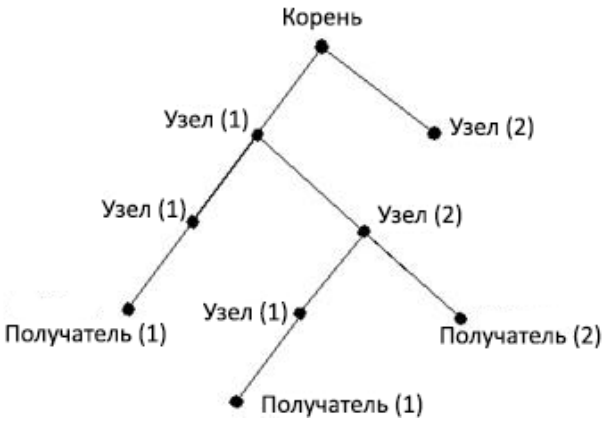


Рис. 108. Структура дерева MIB

9.6.5. Настройка с помощью WEB-интерфейса

1. Включение протокола SNMP и выбор версии.

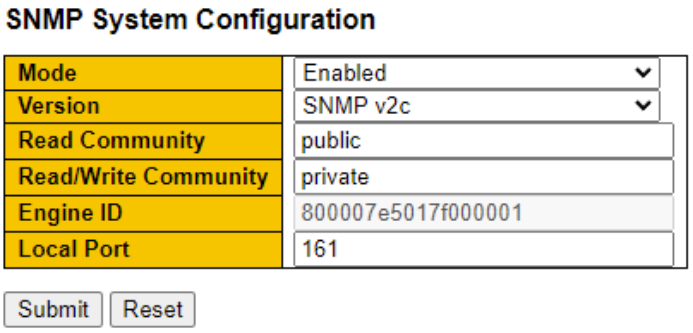


Рис. 109. Включение SNMP

Режим (Mode)
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Enable (Включено)
Описание: включение и выключение протокола SNMP.
Версия 2 (Version)
Опции: SNMP v1/SNMP v2c/SNMP v3
Значение по умолчанию: SNMP v2c
Описание: выбор версии SNMP. Версия SNMP v2c совместима с версией SNMP v1. Версия SNMP v3 совместима с версиями SNMP v2c и SNMP v1.
Сообщество «Только чтение» (Read-Only Community)
Настраиваемый диапазон: 0 ~ 255 символов
Значение по умолчанию: Public (Открытый)
Функция: настройка имени сообщества «Только чтение» (Read-only community).
Описание: информация MIB коммутатора может быть прочитана только в том случае, если имя сообщества, передаваемое пакетом SNMP, совпадает с именем, настроенным на коммутаторе.
Сообщество «Чтение/Запись» (Read/Write Community)
Настраиваемый диапазон: 0 ~ 255 символов
Значение по умолчанию: Private (Закрытый)
Функция: настройка имени сообщества «Чтение/Запись».
Описание: информация MIB коммутатора может быть прочитана и записана только в том случае, если имя сообщества, передаваемое в пакете SNMP, совпадает с именем, настроенным на коммутаторе.

2. Настройка глобального режима сообщений «Trap».

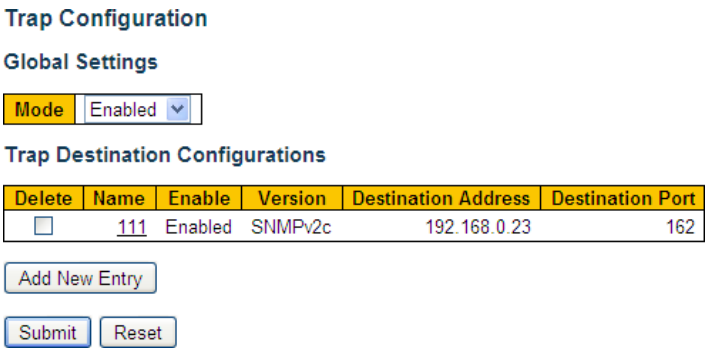


Рис. 110. Настройка глобального режима сообщений «Trap»

Режим (Mode)
Опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Disable (Выключено)
Описание: включение и выключение глобального режима сообщений «Trap».

Нажмите <Add New Entry>, чтобы настроить список сообщений «Trap». Коммутатор поддерживает максимум 4 записи. Нажмите <Name>, чтобы изменить список сообщений «Trap».

3. Настройка списка сообщений «Trap».

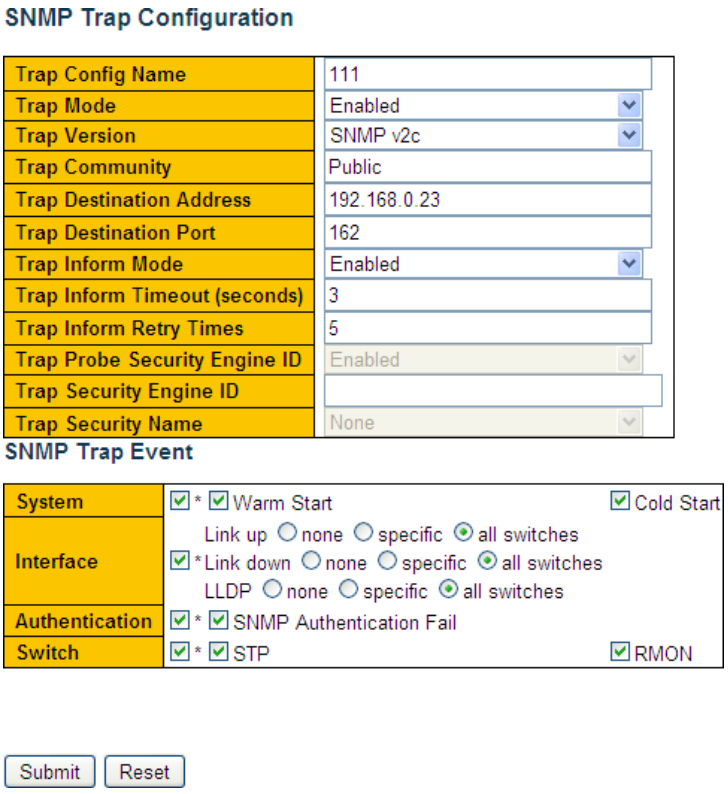


Рис. 111. Настройка списка сообщений «Trap»

Настройка имени списка сообщений «Trap» (Trap Config Name)
Настаиваемый диапазон: 1 ~ 255 сиволов.
Функция: настройка имени списка сообщений «Trap».

Выбор режима сообщений «Trap» (Trap Mode)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение режима сообщений «Trap». После включения данного режима коммутатор может отправлять сообщения «Trap» в NMS.

Версия сообщений «Trap» (Trap Version)
Опции: SNMP v1/SNMP v2c/SNMP v3.
Значение по умолчанию: SNMP v2c
Функция: настройка версии протокола с сообщениями «Trap», отправляемых коммутатором на сервер.

Сообщество сообщений «Trap» (Trap Community)
Настаиваемый диапазон: 1 ~ 255 символов.
Значение по умолчанию: Public (Открытый).
Функция: настройка имени сообщества, которое будет передаваться посредством сообщений «Trap».

Адрес назначения для сообщений «Trap» (Trap Destination Address)
Формат: A.B.C.D
Функция: настройка адреса сервера для приема сообщений «Trap».

Порт назначение для сообщений «Trap» (Trap Destination Port)
Настаиваемый диапазон: 1 ~ 65535.
Значение по умолчанию: 162.
Функция: настройка номера порта для передачи сообщений «Trap».

Режим информирования сообщений «Trap» (Trap Inform Mode)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: настройка функции ответа коммутатору после того, как сервер получит пакет с сообщением «Trap».

Таймаут для режима информирования сообщений «Trap» (Trap Inform Timeout)
Настаиваемый диапазон: 1 ~ 2147 сек.
Значение по умолчанию: 3 сек.
Функция: настройка времени ожидания для отправки пакетов с сообщениями «Trap». После отправки пакета на сервер коммутатор повторно передает пакет с сообщениями «Trap», если он не получает ответа от сервера в течение данного периода.

Количество таймаутов для режима информирования сообщений «Trap» (Trap Inform Retry Times)
Настаиваемый диапазон: 0 ~ 255.
Значение по умолчанию: 5.
Функция: настройка количества таймаутов повторной отправки пакетов с сообщениями «Trap». Если количество повторов превышает значение этого параметра и сервер не отвечает, считается, что передача пакета не удалась.

«Горячий старт»/»Холодный» старт (Warm Start/Cold Start)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: настройка функции передачи пакетов с сообщениями «Trap» при выполнении «Горячего старт»/»Холодного» старта коммутатора.
Связь есть/Связи нет (Link up/ Link down)
Опции: none/specific/all switches.
Значение по умолчанию: none.
Функция: настройка функции передачи пакетов с сообщениями «Trap» при изменении статуса порта.
LLDP
Опции: none/specific/all switches.
Значение по умолчанию: none.
Функция: настройка функции передачи пакетов с сообщениями «Trap» при изменении статуса «соседа».
Ошибка аутентификации SNMP (SNMP Authentication Fail)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: настройка функции отправки сообщений «Trap» при ошибке аутентификации SNMP.
STP
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: настройка функции отправки сообщений «Trap» при изменении статуса STP.

9.6.6. Пример типовой настройки

Управляющий сервер (NMS) SNMP подключается к коммутатору через сеть Ethernet. IP адрес управляющего сервера: 192.168.0.23, а IP адрес коммутатора: 192.168.0.2. NMS управляет и контролирует Агента с помощью протокола SNMPv2, который может читать и записывать информацию MIB Агента. Агент автоматически отправляет сообщения «Trap» в NMS, когда у Агента происходит аварийная ситуация (см. рис. 112).

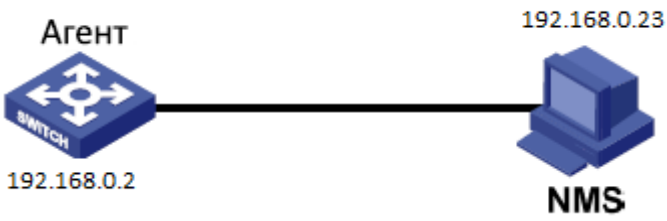


Рис. 112. Пример настройки SNMPv2

Настройка Агента:

- Включите протокол SNMP версии v2; настройте права доступа, установив режим Сообщества только для чтения (Read-only Community) как «Public» и режим Сообщества чтения и записи (Read&write Community) как «Private» (см. рис. 109);
- Включите глобальный режим сообщений «Trap» (см. рис. 110).
- Создайте запись для сообщений «Trap» как 111, включите режим сообщений «Trap»; настройте версию для сообщений «Trap» как SNMP v2c и IP-адрес назначения как 192.168.0.23. Выберите систему, интерфейс, аутентификацию и все сообщения «Trap» для коммутатора, а также установитее настройки по умолчанию для других параметров (см. рис. 111).

Если пользователю необходимо управлять и контролировать Агента, необходимо использовать соответствующее программное обеспечение (NMS).

9.7. Протокол SNMP v3

9.7.1. Введение

SNMPv3 предоставляет собой механизм аутентификации USM (User-Based Security Model). Пользователь может настроить функции шифрования и аутентификации. Аутентификация используется для проверки легальности отправителя сообщения для того, чтобы избежать доступа нелегальных пользователей. SNMPv3 обеспечивает шифрование передаваемых сообщений между NMS и агентом, чтобы избежать их незаконного просмотра. Комбинация аутентификации и шифрования улучшает безопасность связи между SNMP NMS и Агентом SNMP.

Для обеспечения связи между NMS и агентом их версии SNMP должны совпадать. Для агента можно настроить разные версии SNMP, чтобы он мог использовать разные версии для связи с разными NMS.

9.7.2. Реализация

SNMPv3 имеет 4 таблицы конфигурации, для каждой из которых можно создать 16 записей. Эти таблицы определяют, могут ли указанные пользователи получать доступ к информации MIB.

Вы можете создать несколько пользователей в таблице пользователей. Каждый пользователь может использовать разные политики безопасности для реализации функций аутентификации, шифрования и других функций безопасности.

Таблица доступа может обращаться к информации узла MIB, сопоставляя имя группы, контекстное имя и устанавливать соответствующий уровень безопасности.

Групповая таблица - это совокупность нескольких пользователей. Права доступа устанавливаются для группы пользователей и применимы для всех пользователей в группе. Контекстная таблица - это читаемые строки символов для идентификации пользователей. Это не имеет никакого отношения к конкретной модели безопасности.

9.7.3. Настройка с помощью WEB-интерфейса

1. Включение протокола SNMP и выбор версии.

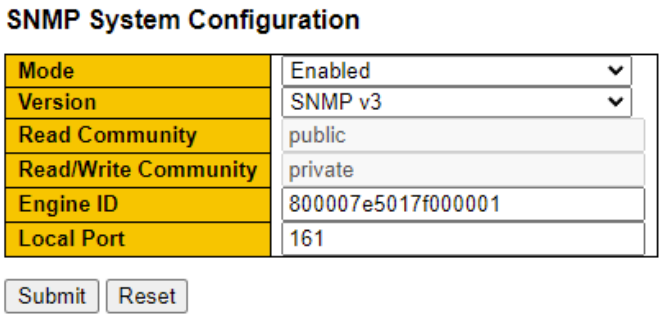


Рис. 113. Включение SNMP

Режим (Mode)
Опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Enable (Включено)
Описание: включение и выключение протокола SNMP.
Версия (Version)
Опции: SNMP v1/SNMP v2c/SNMP v3
Значение по умолчанию: SNMP v2c
Описание: выбор версии SNMP. Версия SNMP v2c совместима с версией SNMP v1. Версия SNMP v3 совместима с версиями SNMP v2c и SNMP v1.
Идентификатор ядра (Engine ID)
Диапазон конфигурации: четное количество шестнадцатиричных чисел, которое не может содержать только все символы «0» или все символы «F»; диапазон четного числа цифр должен быть от 10 до 64.
Функция: настройка идентификатора ядра для системы SNMPv3. Если идентификатор ядра был изменен, пользователи, соответствующие идентификаторам устройств в таблице пользователей, удаляются.

2. Настройка глобального режима сообщений «Trap».

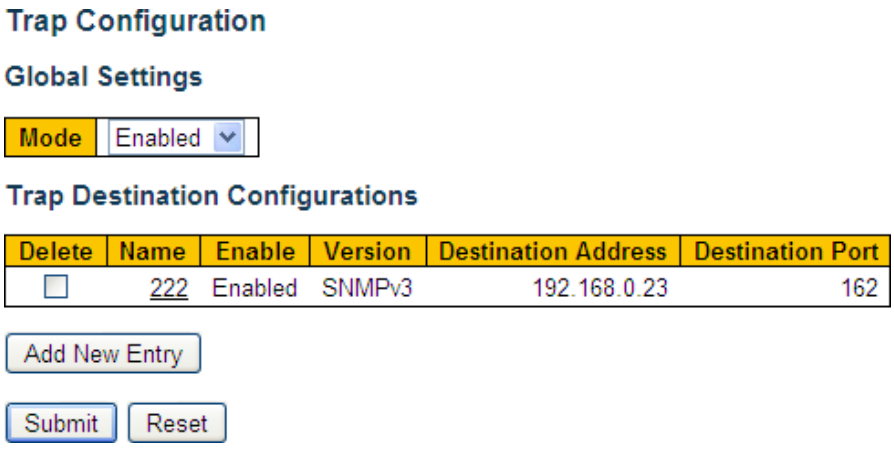


Рис. 114. Настройка глобального режима сообщений «Trap»

Режим (Mode)
Опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Disable (Выключено)
Описание: включение и выключение глобального режима сообщений «Trap».

Нажмите <Add New Entry>, чтобы настроить список сообщений «Trap». Коммутатор поддерживает максимум 4 записи. Нажмите <Name>, чтобы изменить список сообщений «Trap».

3. Настройка списка сообщений «Trap».

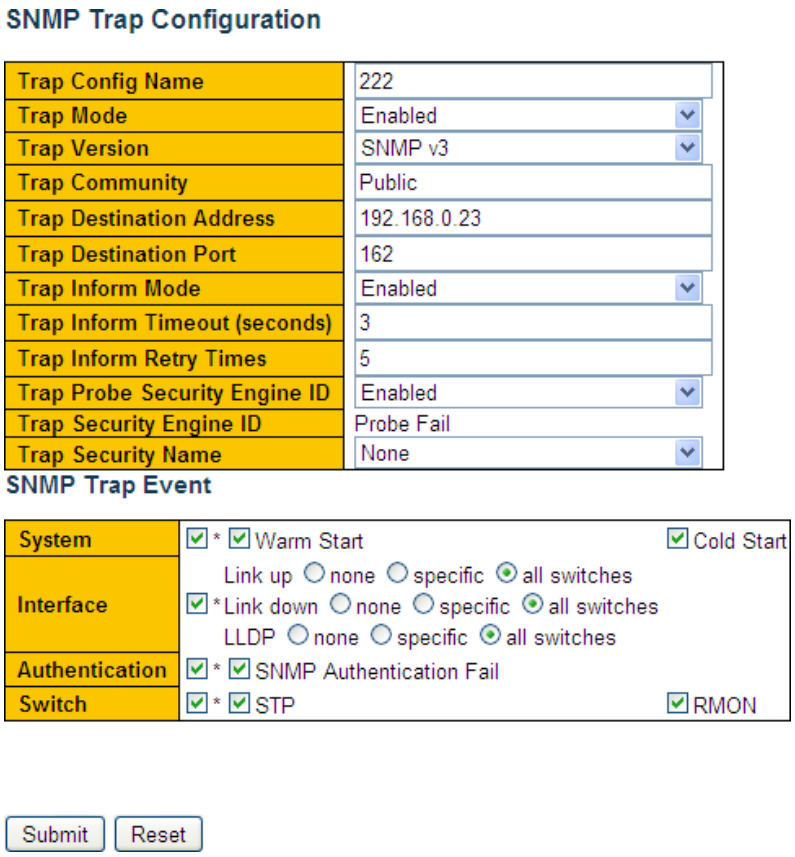


Рис. 115. Настройка списка сообщений «Trap»

Настройка имени списка сообщений «Trap» (Trap Config Name)
Настаиваемый диапазон: 1 ~ 255 сиволов.
Функция: настройка имени списка сообщений «Trap».
Выбор режима сообщений «Trap» (Trap Mode)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение режима сообщений «Trap». После включения данного режима коммутатор может отправлять сообщения «Trap» в NMS.

Версия сообщений «Trap» (Trap Version)
Опции: SNMP v1/SNMP v2c/SNMP v3.
Значение по умолчанию: SNMP v2c
Функция: настройка версии протокола с сообщениями «Trap», отправляемых коммутатором на сервер.

Сообщество сообщений «Trap» (Trap Community)
Настаиваемый диапазон: 1 ~ 255 символов.
Значение по умолчанию: Public (Открытый).
Функция: настройка имени сообщества, которое будет передаваться посредством сообщений «Trap».

Адрес назначения для сообщений «Trap» (Trap Destination Address)
Формат: A.B.C.D
Функция: настройка адреса сервера для приема сообщений «Trap».

Порт назначение для сообщений «Trap» (Trap Destination Port)
Настаиваемый диапазон: 1 ~ 65535.
Значение по умолчанию: 162.
Функция: настройка номера порта для передачи сообщений «Trap».

Режим информирования сообщений «Trap» (Trap Inform Mode)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: настройка функции ответа коммутатору после того, как сервер получит пакет с сообщением «Trap».

Таймаут для режима информирования сообщений «Trap» (Trap Inform Timeout)
Настаиваемый диапазон: 1 ~ 2147 сек.
Значение по умолчанию: 3 сек.
Функция: настройка времени ожидания для отправки пакетов с сообщениями «Trap». После отправки пакета на сервер коммутатор повторно передает пакет с сообщениями «Trap», если он не получает ответа от сервера в течение данного периода.

Количество таймаутов для режима информирования сообщений «Trap» (Trap Inform Retry Times)
Настаиваемый диапазон: 0 ~ 255.
Значение по умолчанию: 5.
Функция: настройка количества таймаутов повторной отправки пакетов с сообщениями «Trap». Если количество повторов превышает значение этого параметра и сервер не отвечает, считается, что передача пакета не удалась.

Проверка безопасности идентификатора ядра сообщений «Trap» (Probe Security Engine ID)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: настройка проверки безопасности идентификатора ядра, передаваемого в сообщениях «Trap» SNMP v3. Если установлено значение «Enable» (Включено), коммутатор автоматически получает и проверяет безопасность идентификатора ядра. Если установлено значение «Disabled» (Выключено), идентификатор системы безопасности формируется из значения Trap Security Engine ID.

Безопасный идентификатор ядра сообщений «Trap» (Trap Security Engine ID)
Настаиваемый диапазон: четное количество шестнадцатиричных чисел, которое не может содержать только все символы «0» или все символы «F»; диапазон четного числа цифр должен быть от 10 до 64.
Функция: настройка безопасного идентификатора ядра, передаваемого в сообщении «Trap».
«Горячий старт»/»Холодный» старт (Warm Start/Cold Start)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: настройка функции передачи пакетов с сообщениями «Trap» при выполнении «Горячего старт»/»Холодного» старта коммутатора.
Связь есть/Связи нет (Link up/ Link down)
Опции: none/specific/all switches.
Значение по умолчанию: none.
Функция: настройка функции передачи пакетов с сообщениями «Trap» при изменении статуса порта.
LLDP
Опции: none/specific/all switches.
Значение по умолчанию: none.
Функция: настройка функции передачи пакетов с сообщениями «Trap» при изменении статуса «соседа».
Ошибка аутентификации SNMP (SNMP Authentication Fail)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: настройка функции отправки сообщений «Trap» при ошибке аутентификации SNMP.
STP
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: настройка функции отправки сообщений «Trap» при изменении статуса STP.

4. Настройка Сообществ SNMP v3.

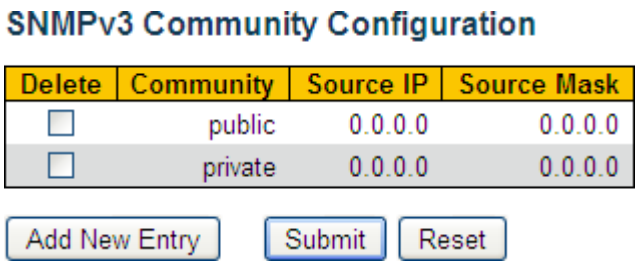


Рис. 116. Настройка сообществ SNMP v3

Сообщества (Community)
Настаиваемый диапазон: 1 ~ 32 символов.

Функция: создание имени Сообщества.
Когда выбран протокол SNMP v3, можно задать имя Сообщества, чтобы разрешить системе управления сетью (NMS) получить доступ к коммутатору через SNMPv1 и SNMPv2. В этом случае имя Сообщества в NMS должно соответствовать имени Сообщества на коммутаторе. Права доступа каждого Сообщества зависят от конфигурации групповых таблиц и таблицы доступа.

IP-адрес источника (Source IP)
Формат: A.B.C.D
Функция: настройка IP-адреса NMS.

Маска подсети источника (Source Mask)
Формат: A.B.C.D
Функция: вы можете настроить пул диапазона IP-адресов. Диапазон адресов определяется маской подсети. Маска подсети - это число длиной 32 бита, состоящее из строки 1 и строки 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста.
Нажмите <Add New Entry>, чтобы настроить Сообщества. Коммутатор поддерживает максимум 16 Сообществ.

По умолчанию существуют имена Сообществ «Public» и «Private». В NMS нет ограничений по IP-адресу.

5. Настройка таблицы пользователей.

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
☐	800007e5017f000001	1111	Auth, Priv	MD5	••••••••	DES	••••••••
☐	800007e5017f000001	2222	Auth, Priv	SHA	••••••••	AES	••••••••

Add New Entry | Submit | Reset

Рис. 117. Настройка сообществ SNMP v3

Идентификатор ядра (Engine ID)
Диапазон конфигурации: четное количество шестнадцатиричных чисел, которое не может содержать только все символы «0» или все символы «F»; диапазон четного числа цифр должен быть от 10 до 64.
Функция: настройка идентификатора ядра пользователя. Если идентификатор ядра пользователя отличается от идентификатора ядра системы SNMPv3, пользователь является недействующим.

Имя пользователя (User Name)
Настаиваемый диапазон: 1 ~ 32 символов.
Функция: создание имени пользователя.

LLDP
Опции: none/specific/all switches.
Значение по умолчанию: none.
Функция: настройка функции передачи пакетов с сообщениями «Trap» при изменении статуса «соседа».

Уровень безопасности (Security Level)
Опции: NoAuth,NoPriv/Auth,NoPriv/Auth,Priv
Функция: настройка уровня безопасности для текущего пользователя.
Описание: NoAuth,NoPriv означает, что ни аутентификация, ни шифрование не требуются. Auth,NoPriv означает, что требуется только аутентификация, без шифрования. Auth,Priv означает, что требуются как аутентификация, так и шифрование.

Протокол аутентификации (Authentication Protocol)
Опции: MD5/SHA
Функция: выбор протокола аутентификации. Необходимо выполнить настройки протокола аутентификации и пароля, когда для уровня безопасности выбраны режимы Auth,NoPriv/AuthPriv.

Пароль аутентификации (Authentication password)
Диапазон настроек: 8~40 символов (протокол MD5), 8~32 символов (протокол SHA)
Функция: создание пароля.

Протокол конфиденциальности (Privacy Protocol)
Опции: DES/AES
Функция: Выбор протокола конфиденциальности. Необходимо выполнить настройки протокола конфиденциальности и пароля, когда выбран режим Auth,Priv.

Пароль конфиденциальности (Privacy Password)
Диапазон настроек: 8~32 символов
Функция: создание пароля конфиденциальности.

По умолчанию в коммутаторе существует пользователь default_user, а уровень безопасности - NoAuth,NoPriv. Поддерживается максимум до 16 пользователей.

6. Настройка групповой таблицы.

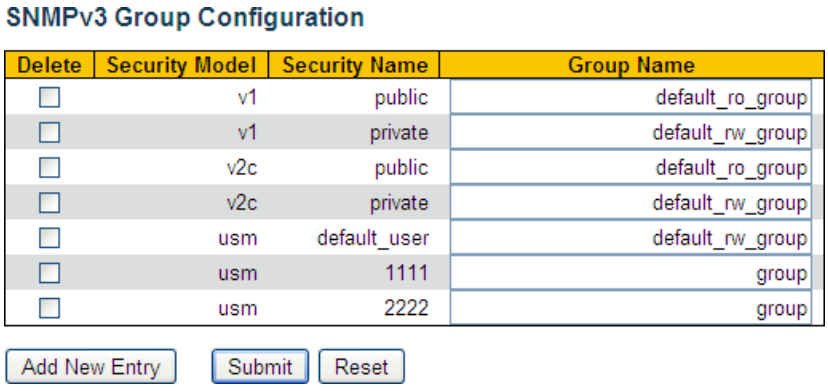


Рис. 118. Настройка групповой таблицы SNMP v3

Модель безопасности (Security model)
Опции: v1/v2/usm
Функция: Выбор модели безопасности для текущей группы (номер версии SNMP). Протокол SNMPv3 использует технологию USM, что является обязательным для реализации модели SNMPv3.
Имя безопасного пользователя (Security Name)
Диапазон настроек: все существующие сообщества/имена пользователей, 1 ~ 32 символа.
Функция: настройка имени безопасного пользователя. Если используется модель безопасности v1/v2, имя должно совпадать с именем Community. Если модель безопасности - usm, имя должно совпадать с именем пользователя в таблице пользователей.
Имя группы (Group Name)
Диапазон настроек: 1 ~ 32 символов
Функция: настройка имени группы. Пользователи с одним и тем же именем группы принадлежат к одной и той же группе.

По умолчанию в коммутаторе существуют следующие групповые таблицы: {v1, public, default_ro_group}, {v1, private, default_rw_group}, {v2c, public, default_ro_group}, {v2c, private, default_rw_group} и {usm, default_user, default_rw_group}. Поддерживается максимум до 16 групп.

7. Настройка таблицы отображения.

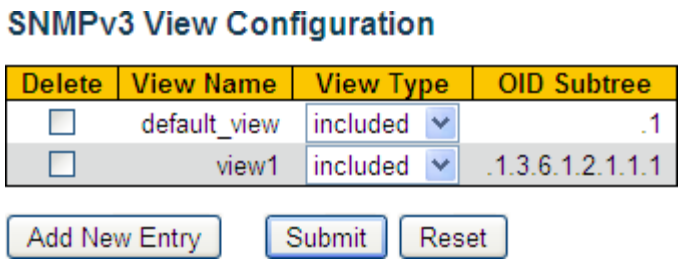


Рис. 119. Настройка таблицы отображения SNMPv3

Просмотр имени (View Name)
Диапазон настройки: 1~32 символов
Функция: настройка отображения имени.
Тип отображения (View Type)
Опции: Included/Excluded (добавлен/исключен)
Функция: опция Included обеспечивает отображение всех узлов поддерева MIB. Опция Excluded не отображает никакой из узлов поддерева MIB.
Идентификатор объекта (OID)
Функция: настройка поддерева MIB, представленного идентификатором объекта корневого узла. Можно настроить до 16 вариантов.

По умолчанию в коммутаторе отображается default_view, и это отображение охватывает все узлы в поддереве. Поддерживается максимум до 16 записей.

8. Настройка таблицы доступа.

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view	None
☐	default_rw_group	any	NoAuth, NoPriv	default_view	default_view
☐	group	usm	Auth, NoPriv	default_view	None

Add New Entry | Submit | Reset

Рис. 120. Настройка таблицы доступа SNMPv3

Имя группы (Group Name)
Диапазон настроек: 1~32 символов
Описание: все пользователи группы обладают одинаковыми полномочиями доступа.
Модель безопасности (Security model)
Настройки по умолчанию: any/v1/v2/usm
Функция: выбор модели безопасности (т.е. номер версии SNMP), которая используется, для доступа к коммутатору. SNMPv3 поддерживает технологию USM. «Any» означает, что применяться может любая модель безопасности. Имя группы и модель защиты должны соответствовать имени группы и модели защиты в групповой таблице.
Уровень безопасности (Security Level)
Опции: NoAuthNoPriv/AuthNoPriv/AuthPriv
Функция: настройка уровня безопасности для текущей группы.
Описание: Для NoAuth,NoPriv не используются ни протокол аутентификации, ни шифрование. Auth,NoPriv означает, что требуется протокол аутентификации, а шифровани не требуется. Auth,Priv означает, что требуется как протокол аутентификации, так и шифрование. Пользователь может получить доступ к указанной информации MIB, только если протокол аутентификации / шифрования и пароль аутентификации / шифрования идентичны тем, которые настроены в таблице пользователей.
NoAuth,NoPriv, Auth,NoPriv, Auth,Priv: уровни безопасности указаны в порядке возрастания. Высокому уровню безопасности разрешается доступ к низкому уровню безопасности. Например, если уровень безопасности группы установлен как AuthNo,Priv, пользователи в группе с уровнями защиты AuthNo,Priv и Auth,Priv могут успешно получить доступ к коммутатору, если оба протокола аутентификации/конфиденциальности и пароли для аутентификации/защиты конфиденциальности соответствуют правилам. При этом пользователи с уровнями безопасности NoAuth,NoPriv доступа не имеют.
Приоритет доступа «Только чтение» (Read View Name)
Опции: default_view/None/all existing view names
Функция: выбор имени для приоритета доступа «Только чтение» (ReadOnly).

Приоритет доступа «Чтение-Запись» (Write View Name)
Опции конфигурации: default_view/None/Created view name
Функция: выбор имени для приоритета доступа «Чтение-запись» (ReadWrite).

По умолчанию в коммутаторе существуют следующие таблицы доступа: {default_ro_group, any, NoAuth,NoPriv, default_view, None} and {default_rw_group, any, NoAuth,NoPriv, default_view, default_view}. Поддерживается максимум до 16 записей.

9.7.4. Пример типовой настройки

Управляющий сервер (NMS) SNMP подключается к коммутатору через сеть Ethernet. IP адрес управляющего сервера: 192.168.0.23, а IP-адрес коммутатора: 192.168.0.2 Пользователь 1111 и пользователь 2222 управляют Агентом через SNMP v3. Уровень безопасности установлен на AuthNoPriv, и коммутатор может выполнять операцию только для чтения для всей информации об узлах Агента. При возникновении аварийного сигнала агент заранее отправляет в NMS сообщения trap v3, как показано на рисунке 123. (см. рис. 112).

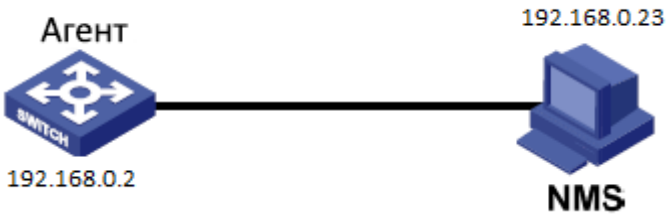


Рис. 121. Пример настройки SNMPv3

Настройка Агента:

- Включите протокол SNMP v3;
- Настройте таблицу пользователей SNMP v3;

Имя пользователя: 1111. Уровень защиты Auth,Priv. Протокол аутентификации: MD5. Пароль аутентификации: aaaaaaaa. Протокол безопасности: DES. Пароль безопасности: xxxxxxxx.

Имя второго пользователя: 2222. Уровень защиты: Auth,Priv. Протокол аутентификации: SHA. Пароль аутентификации: bbbbbbbb. Протокол безопасности: AES. Пароль безопасности: yyyyyyyy. (см. рис. 117).

- Создайте группу, настройте модель безопасности как usm, добавьте пользователей 1111 и 2222 в группу (см. рис. 118);
- Настройте таблицу доступа SNMPv3.

Имя группы: group, модель безопасности: USM, уровень защиты: Auth,NoPriv, приоритет доступа «Read View»: default_view, приоритет доступа «Write View»: None (см. рис. 120);

- Включите глобальный режим сообщений «Trap» (см. рис. 114).
- Создайте элемент таблицы сообщений «Trap» как 222, включите режим сообщений «Trap»; настройте версию для сообщений «Trap» как SNMP v3 и IP-адрес назначения как 192.168.0.23. Выберите систему, интерфейс, аутентификацию и все сообщения «Trap» для коммутатора, а также установите настройки по умолчанию для других параметров (см. рис. 115).

Если пользователю необходимо управлять и контролировать Агента, необходимо использовать соответствующее программное обеспечение (NMS).

9.8. Протокол RMON (Remote Network Monitoring)

9.8.1. Введение

Протокол RMON (Remote Network Monitoring) основан на архитектуре SNMP и позволяет сетевым устройствам управления более интенсивно контролировать устройства. реализация протокола RMON основана на модели клиент/сервер и включает NMS (Network Management Station, Станция управления сетью), по сути являющейся сервером и специального Агента (Agent), который является клиентом. NMS управляет Агентом, который выполняет сбор статистики о трафике на порту.

Основные функции RMON – сбор статистики и сигнализация о тревогах. Функция сбора статистики предполагает, что агент может периодически выполнять сбор статистики всех видов информации о трафике на порте, например, получение информации о количестве сообщений, полученных в конкретном сегменте сети в течение конкретного периода времени. Функция сигнализации о тревогах обеспечивает выполнение агентом функций контроля за значениями указанных переменных MIB (Management Information Base) файлов. Когда значение достигает определенного порога (например, количество сообщений превышает указанное значение), агент может автоматически записывать события тревоги в журнал RMON или отправлять специальные Trap-сообщение на устройство управления.

9.8.2. Группы RMON (RMON Group)

Протокол RMON (стандарт RFC2819) подразделяется на несколько групп, которые включают: группу статистики (Statistics Group), группу истории (History Group), группу событий (Event Group) и группу тревог (Alarm Group) открытых MIB. Каждая группа поддерживает максимум 32 записи.

- Группа статистики (Statistics Group)

Наличие данной группы подразумевает, что система может вести сбор статистики всех видов информации о трафике на порту. Статистическая информация содержит много разной информации: количество коллизий в сети, сообщения об ошибках CRC, информацию о сообщениях со слишком маленьким или слишком большим размерами данных, информацию о широковещательных и многоадресных сообщениях, количество полученных байт, количество принятых сообщений и т.д. После успешного создания записи статистики по указанному интерфейсу, данная группа подсчитывает количество

сообщений на текущем интерфейсе, а результатом является непрерывное накопление значений статистики.

- Группа истории (History Group)

Система периодически просматривает выборку всех видов информации о трафике на порту и сохраняет значения выборки в таблице записей истории, следовательно устройство управления может просматривать эту информацию в любое время. Группа истории учитывает значения статистики всех видов данных в интервале выборки сообщений, полученных портом в каждом цикле приема/передачи информации, причем периодичность данных циклов можно настраивать.

- Группа событий (Event group)

Группа событий используется для определения индексов событий и методов обработки событий. События, обработанные в группе событий, используются в элементе конфигурации группы тревог. Действие события начинается, когда контролируемое устройство достигает состояния тревоги.

Существует несколько способов обработки событий:

Журнал (Log): ведение журнала события и связанной с ним информации;

Прерывание (Trap): отправка Trap-сообщения в NMS и дальнейшее информирование о событии;

Log-Trap: запись и отправка Trap-сообщения;

Нет (None): не выполнять никаких действий

- Группа тревожной сигнализации (Alarm Group)

Функция управления тревожной сигнализацией протокола RMON обеспечивает контроль за определенными тревогами. После того, как пользователь обнаружит записи тревоги, система будет получать значения контролируемых переменных сигнала тревоги за определенный период. Когда значение переменной сигнала тревоги больше или равно пороговому значению, пользователь будет информирован о важной тревоге. Когда значение переменной тревоги ниже порогового значения, пользователь будет информирован о второстепенной тревоге. Тревоги будут обрабатываться в соответствии с определением конкретного события.

Если выборочное значение переменной аварийного сигнала превышает пороговое значение несколько раз в одном и том же направлении, инициирование события о тревоге возможно только первый раз. Это означает, что увеличение количества тревог и уменьшение количества тревог чередуются.

9.8.3. Настройка через WEB-интерфейс

1. Настройка таблицы статистики.

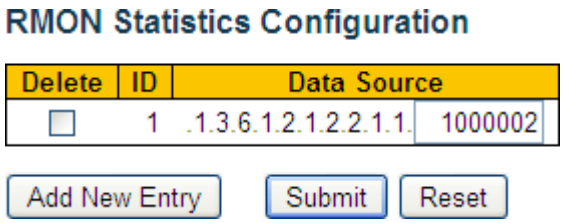


Рис. 122. Настройка статистики RMON

Идентификатор (ID)

Настраиваемый диапазон: 1~65535

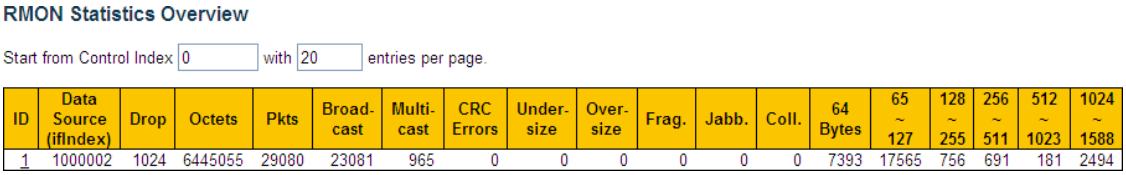
Описание: настройка номера записи статистики. Группа статистики поддерживает до 128 записей.

Источник данных (Data Source)

Настраиваемый диапазон: 100000portid

Описание: Выбор порта для сбора статистики.

2. Отображение статуса статистики группы.



ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
1	1000002	1024	6445055	29080	23081	965	0	0	0	0	0	0	7393	17565	756	691	181	2494

Рис. 123. Настройка статистики RMON

Drop: количество пакетов, отброшенных портом.

Octets: количество байтов, полученных портом.

Pkts: количество пакетов, полученных портом.

Broadcast: количество широковещательных пакетов, полученных портом.

Multicast: количество многоадресных пакетов, полученных портом.

CRC Errors: количество пакетов с ошибками CRC длиной от 64 до 9600 байт, полученных портом.

Undersize: количество пакетов размером менее 64 байт, полученных портом.

Oversize: количество пакетов размером более 9600 байт, полученных портом.

Frag: количество пакетов с ошибкой CRC, содержащих менее 64 байтов, полученных портом.

Jabb .: количество пакетов с ошибкой CRC, содержащих более 9600 байт, полученных портом.

Coll .: количество конфликтов, полученных портом в полудуплексном режиме.

64 Bytes: количество пакетов длиной 64 байта, полученных портом.

65 ~ 127: количество пакетов длиной от 65 до 127 байт, полученных портом.

128 ~ 255: количество пакетов длиной от 128 до 255 байт, полученных портом.

256 ~ 511: количество пакетов длиной от 256 до 511 байт, полученных портом.

512 ~ 1023: количество пакетов длиной от 512 до 1023 байтов, полученных портом.

1024 ~ 1588: количество пакетов длиной от 1024 до 1588 байт, полученных портом.

Значение Oversize (превышение размера) зависит от параметра «Maximum Frame Size» (максимальный размер кадра) в конфигурации порта.

3. Настройка таблицы истории.

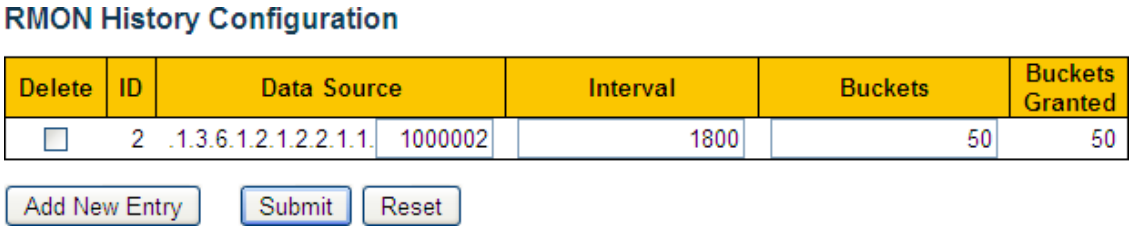
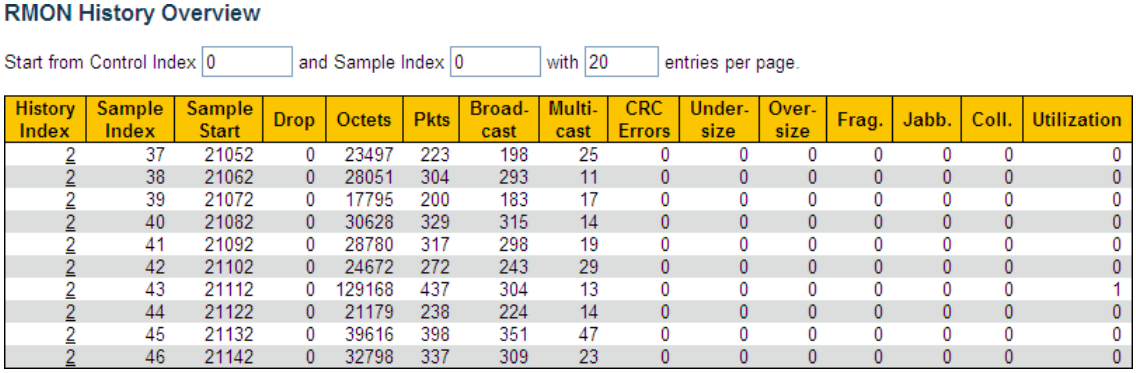


Рис. 124. Настройка истории RMON

Идентификатор (ID)
Настраиваемый диапазон: 1 ~ 65535
Функция: настройка количества записей истории. Поддерживается максимум до 256 записей.
Источник данных (Data Source)
Опции: 100000portid
Функция: настройка порта для записей истории.
Интервал выборки (Interval)
Настраиваемый диапазон (сек.): 1 ~ 3600 сек.
Функция: настройка интервала выборки.
Количество значений (Buckets)
Настраиваемый диапазон: 1 ~ 65535
Функция: настройка количества последних значений записей истории.

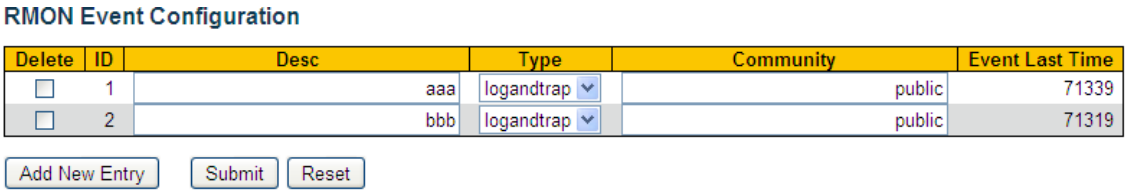
4. Просмотр информации записей истории.



History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
2	37	21052	0	23497	223	198	25	0	0	0	0	0	0	0
2	38	21062	0	28051	304	293	11	0	0	0	0	0	0	0
2	39	21072	0	17795	200	183	17	0	0	0	0	0	0	0
2	40	21082	0	30628	329	315	14	0	0	0	0	0	0	0
2	41	21092	0	28780	317	298	19	0	0	0	0	0	0	0
2	42	21102	0	24672	272	243	29	0	0	0	0	0	0	0
2	43	21112	0	129168	437	304	13	0	0	0	0	0	0	1
2	44	21122	0	21179	238	224	14	0	0	0	0	0	0	0
2	45	21132	0	39616	398	351	47	0	0	0	0	0	0	0
2	46	21142	0	32798	337	309	23	0	0	0	0	0	0	0

Рис. 125. Информация записей истории RMON

5. Настройка таблицы событий.


RMON Event Configuration

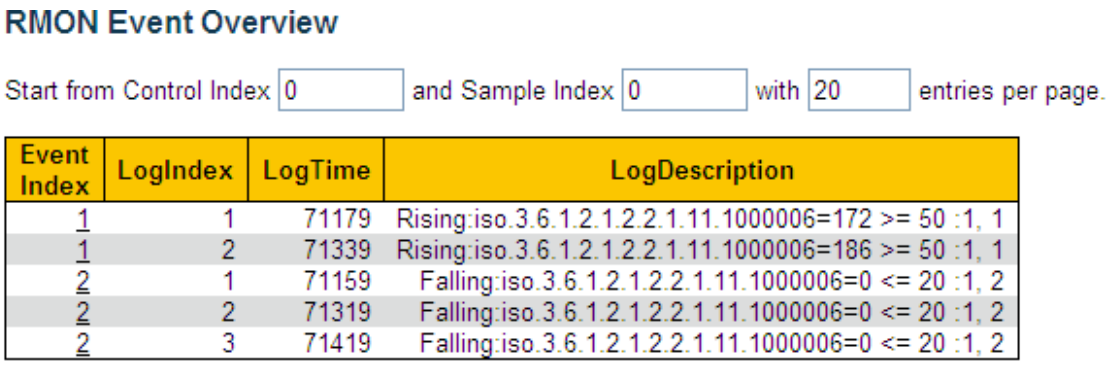
Delete	ID	Desc	Type	Community	Event Last Time
☐	1	aaa	logandtrap	public	71339
☐	2	bbb	logandtrap	public	71319

Add New Entry | Submit | Reset

Рис. 126. Информация таблицы событий

Идентификатор (ID)
Настраиваемый диапазон: 1 ~ 65535
Функция: настройка порядкового номера записи события. Группа событий поддерживает до 128 записей.
Описание (Desc)
Настраиваемый диапазон: 1 ~ 127 символов
Функция: описание событий.
Тип события (Event Type)
Опции: none/log/snmptrap/logandtrap
Значение по умолчанию: none
Функция: настройка типа события при возникновении тревог, т.е. метод обработки сигналов тревоги.
Сообщество (Community)
Настраиваемый диапазон: 1 ~127 символов
Значение по умолчанию: public
Функция: настройка имени сообщества для отправки событий сообщения «Trap». Значение должно быть идентично значению в SNMP.
Время последнего события (Event Last Time)
Функция: отображает значение sysUpTime, если событие используется в последний раз.

6. Просмотр статуса событий группы.

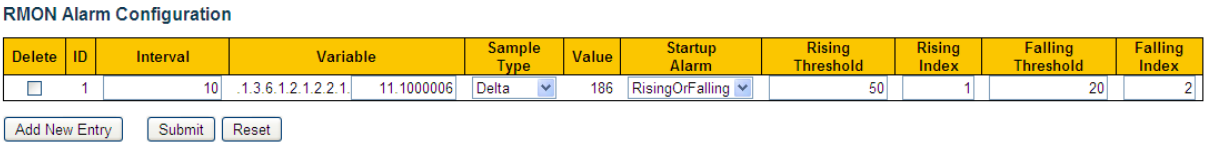

RMON Event Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

Event Index	LogIndex	LogTime	LogDescription
1	1	71179	Rising:iso.3.6.1.2.1.2.2.1.11.1000006=172 >= 50 :1, 1
1	2	71339	Rising:iso.3.6.1.2.1.2.2.1.11.1000006=186 >= 50 :1, 1
2	1	71159	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2
2	2	71319	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2
2	3	71419	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2

Рис. 127. Информация таблицы событий

7. Настройка таблицы тревог.


RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
☐	1	10	.1.3.6.1.2.1.2.2.1.11.1000006	Delta	186	RisingOrFalling	50	1	20	2

Add New Entry | Submit | Reset

Рис. 128. Настройка таблицы тревог

Идентификатор (ID)
Настраиваемый диапазон: 1 ~ 65535
Функция: настройка количества записей тревог. Группа поддерживает до 256 записей.
Интервал (Interval)
Настраиваемый диапазон (сек.): 1 ~ 2147483647 сек.
Значение по умолчанию: 30 сек.
Функция: настройка интервала выборки.
Интервал (Interval)
Формат: A.100000portid
Настраиваемый диапазон: A: 10 ~ 21
Функция: выбор информации порта MIB, которую нужно отслеживать.
InOctets: A=10, количество байтов, полученных портом.
InUcastPkts: A=11, количество одноадресных пакетов, полученных портом.
InNUcastPkts: A=12, количество широковещательных и многоадресных пакетов, полученных портом.
InDiscards: A=13, количество пакетов, отброшенных портом.
InErrors: A=14, количество пакетов с ошибками, полученных портом.
InUnknownProtos: A=15, количество неизвестных пакетов, полученных портом.
OutOctets: A=16, количество байтов, отправленных портом.
OutUcastPkts: A=17, количество одноадресных пакетов, отправленных портом.
OutNUcastPkts: A=18, количество широковещательных и многоадресных пакетов, отправленных портом.
OutDiscards: A=19, количество отброшенных пакетов, отправленных портом.
OutErrors: A=20, количество пакетов с ошибками, отправленных портом.
OutQLen: A=21, длина пакетов в очереди исходящего порта.
Тип выборки (Sampling Type)
Настраиваемые опции: Absolute/Delta
Значение по умолчанию: Delta
Функция: выбор метода сравнения значения выборки и порога.
Absolute: прямое сравнение каждого значения выборки с порогом;
Delta: текущее значение выборки минус предыдущее значение выборки, затем используется разница для сравнения с порогом.
Тип аварийной сигнализации (Startup Alarm)
Настраиваемые опции: Rising/Falling/RisingOrFalling
Значение по умолчанию: RisingOrFalling

Функция: выбор типа аварийной сигнализации.

Верхнее пороговое значение (Rising Threshold)

Настраиваемый диапазон: 1 ~ 2147483647

Функция: настройка верхнего порогового значения. Если значение выборки превышает пороговое значение, а тип сигнала тревоги установлен как RisingAlarm или RisOrFallAlarm, тревога будет активирована, кроме того активируется индекс роста событий.

Индекс роста (Rising Index)

Настраиваемый диапазон: 1 ~ 65535

Функция: настройка возрастающего индекса событий. Это метод передачи возрастания тревог.

Нижнее пороговое значение (Falling Threshold)

Настраиваемый диапазон: 1 ~ 2147483647

Функция: настройка нижнего порогового значения. Когда значение выборки ниже порогового значения, а тип сигнала тревоги установлен как FallingAlarm или RisOrFallAlarm, тревога будет активирована, кроме того активируется индекс снижения события.

Индекс снижения (Falling Index)

Настраиваемый диапазон: 0~65535

Функция: настройка индекса снижения событий. Это метод передачи снижения тревог.

8. Отображение статуса групповых тревог.

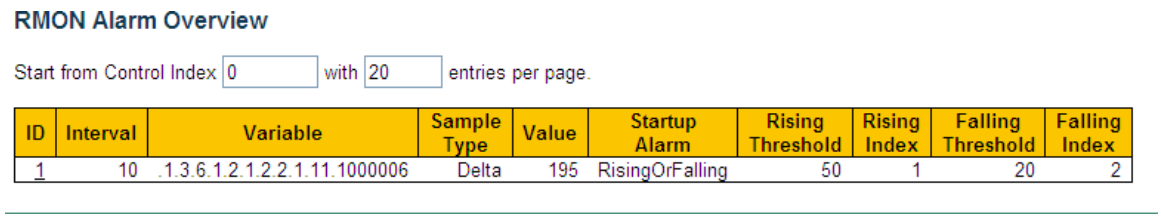


Рис. 129. Отображение статуса групповых тревог

9.9. Настройка TACACS+

9.9.1. Введение

Сеансовый протокол TACACS+ является приложением на основе протокола TCP. Он поддерживает режим клиент/сервер для реализации соединения между Сервером Сетевого Доступа (NAS) и TACACS+ сервером. Клиент работает на сервере NAS, а сервер осуществляет централизованное управление информацией о пользователе. Сервер NAS служит сервером для пользователей и клиентом для сервера. Структура показана на рис. 130.

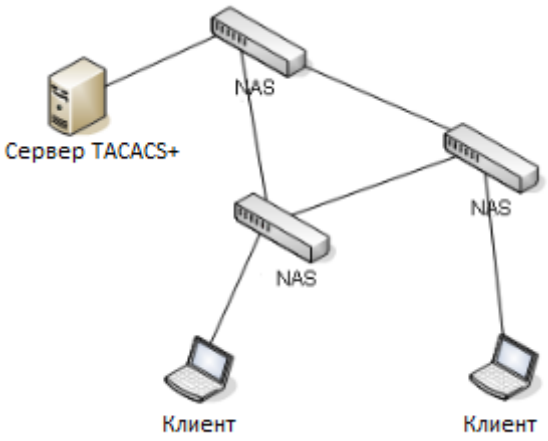


Рис. 130. Структура TACACS+

Протокол осуществляет аутентификацию, авторизацию и опрашивает конечных пользователей, которым необходимо войти в систему. Устройство пользователя действует как TACACS+ клиент и отправляет имя пользователя и пароль на TACACS+ сервер для аутентификации. Сервер получает TCP запросы о подключении от пользователей, отвечает на запросы об аутентификации и проверяет права пользователей. Если пользователь проходит процесс аутентификации, он получает доступ в систему для работы.

9.9.2. Настройка через WEB-интерфейс

1. Настройка глобальных параметров TACACS+

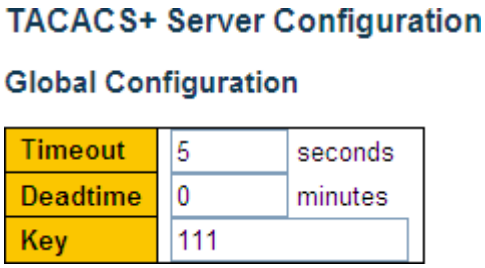


Рис. 131. Настройка глобальных параметров TACACS+

Таймаут (Timeout)
Настраиваемый диапазон (сек.): 1 ~ 1000 сек.
Значение по умолчанию: 5 сек.
Функция: настройка времени таймаута для ответа от сервера TACACS +. Если устройство не получит ответа от сервера TACACS+ после указанного времени, аутентификация не выполняется, и устройство будет считать, что сервер TACACS+ не рабочий.
Нерабочее время (Deadtime)
Настраиваемый диапазон (сек.): 1 ~ 1440 мин.
Значение по умолчанию: 0 мин.

Функция: настройка периода, когда сервер является недействующим. В течение этого периода устройство не отправляет на сервер TACACS+ сообщения с запросом. Параметр «0» - отключение функции. Вы можете включить эту функцию, только если настроено более одного сервера TACACS +.

Ключ шифрования (Key)

Настраиваемый диапазон: 0 ~ 63 символов

Функция: настройка значения ключа шифрования для повышения безопасности связи между клиентом и сервером TACACS+. Для проверки достоверности передаваемых данных, два устройства должны иметь один и тот же ключ шифрования. Таким образом, необходимо убедиться в том, что ключ клиента соответствует ключу, записанному на сервере TACACS+.

2. Настройка сервера TACACS+.

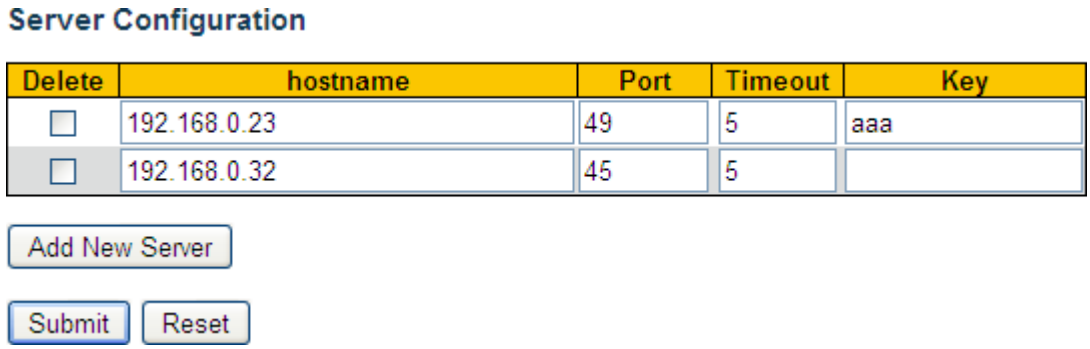


Рис. 132. Настройка сервера TACACS+

Имя хоста (Hostname)

Функция: настройка IP-адреса или имени хоста сервера TACACS+. Максимально может быть настроено 5 серверов TACACS+.

Порт (Port)

Настраиваемый диапазон (сек.): 1 ~ 65535.

Значение по умолчанию: 49.

Функция: настройка порта TCP сервера TACACS+ для аутентификации.

Таймаут (Timeout)

Настраиваемый диапазон (сек.): 1 ~ 1000 сек.

Значение по умолчанию: 5 сек.

Функция: настройка времени таймаута для ответа от сервера TACACS +. Если устройство не получит ответа от сервера TACACS+ после указанного времени, аутентификация не выполняется, и устройство будет считать, что сервер TACACS+ не рабочий.

Ключ шифрования (Key)

Настраиваемый диапазон: 0 ~ 63 символов

Функция: настройка значения ключа шифрования для повышения безопасности связи между клиентом и сервером TACACS+. Для проверки достоверности передаваемых данных, два устройства должны иметь один и тот же ключ шифрования. Таким образом,

необходимо убедиться в том, что ключ клиента соответствует ключу, записанному на сервере TACACS+.

Настройки приоритета значений “Timeout” и “Key” для сервера TACACS+ в данном разделе выше, чем настройки в глобальной конфигурации TACACS+.

9.9.3. Пример типовой настройки

Сервер TACACS+ обеспечивает аутентификацию а авторизацию пользователей при подключении к коммутатору. IP-адрес сервера 192.168.0.23, а общий ключ, используемый при обмене пакетами между коммутатором и сервером – «aaa».

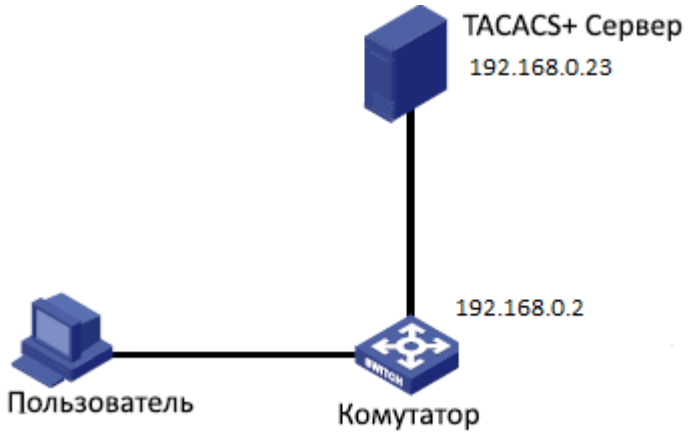


Рис. 133. Пример аутентификации TACACS+

1. Настройте сервер TACACS+. IP-адрес сервера настройте как 192.168.0.23, а ключ как «aaa» (см. рис. 132).
2. При входе в коммутатор через Интернет выберите «Local», при входе в коммутатор через telnet выберите «Tacacs+» (см. рис. 94).
3. Настройте имя пользователя и пароль «bbb», зашифруйте ключ «aaa» на сервере TACACS+.
4. При входе на коммутатор через Интернет введите имя пользователя «admin» и пароль «123», чтобы пройти локальную аутентификацию.
5. При входе в коммутатор через Telnet введите имя пользователя и пароль «bbb» для прохождения аутентификации на сервере TACACS+.

9.10. Настройка RADIUS

9.10.1. Введение

RADIUS (Служба удаленной аутентификации пользователей) является распространенным протоколом передачи данных. Он определяет формат RADIUS кадра на основе UDP и механизм передачи данных, гарантируя защиту сетей от несанкционированного доступа. Как правило, RADIUS используется в сетях с высокими требованиями безопасности и удаленным доступом пользователей.

RADIUS поддерживает режим клиент/сервер, обеспечивая соединение между NAS (Сервером сетевого доступа) и RADIUS сервером. RADIUS клиент работает на NAS сервере. RADIUS сервер осуществляет централизованное управление информацией о пользователе. NAS сервер выполняет функции сервера для пользователей и функции клиента для RADIUS сервер. На Рисунке 92 показана структура.

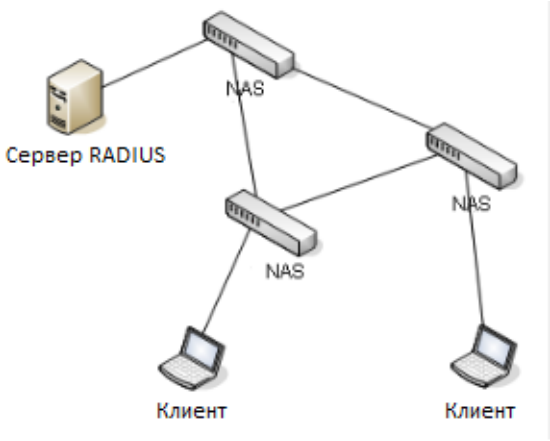


Рис. 134. Структура RADIUS

Протокол проводит аутентификацию конечных пользователей, которым необходимо авторизоваться в системе устройства для работы. Действуя как RADIUS клиент, устройство отправляет информацию о пользователе на RADIUS сервер для аутентификации и разрешает или запрещает пользователям войти в систему устройства по результатам процесса аутентификации.

9.10.2. Настройка через WEB-интерфейс

1. Настройка глобальных параметров протокола RADIUS

RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key	111	
NAS-IP-Address	192.168.0.220	
NAS-IPv6-Address		
NAS-Identifier	222	

Рис. 135. Настройка глобальных параметров RADIUS

Таймаут (Timeout)
Настраиваемый диапазон (сек.): 1 ~ 1000 сек.

Значение по умолчанию: 5 сек.
Функция: настройка времени таймаута для ответа от сервера RADIUS. После отправки запроса на сервер RADIUS устройство повторно отправляет запрос на сервер RADIUS после указанного времени, в случае, если от сервера RADIUS ответа нет.

Количество повторов (Retransmit)
Настраиваемый диапазон (сек.): 1 ~ 1000.
Значение по умолчанию: 3.
Функция: настройка максимального количества попыток повторной передачи запросов на сервер RADIUS. Если устройство по-прежнему не получает ответных пакетов от сервера RADIUS после максимального количества попыток повторной передачи, аутентификация не выполняется, и устройство считает, что сервер RADIUS не рабочий.

Нерабочее время (Deadtime)
Настраиваемый диапазон (сек.): 1 ~ 1440 мин.
Значение по умолчанию: 0 мин.
Функция: настройка периода, когда сервер является недействующим. В течение этого периода устройство не отправляет на сервер RADIUS сообщения с запросом. Параметр «0» - отключение функции. Вы можете включить эту функцию, только если настроено более одного сервера RADIUS.

Ключ шифрования (Key)
Настраиваемый диапазон: 0 ~ 63 символов
Функция: настройка значения ключа шифрования для повышения безопасности связи между клиентом и сервером RADIUS. Для проверки достоверности передаваемых данных, два устройства должны иметь один и тот же ключ шифрования. Таким образом, необходимо убедиться в том, что ключ клиента соответствует ключу, записанному на сервере RADIUS.

IP-адрес NAS (NAS-IP-Address)
Функция: настройка IP-адреса источника, который используется оборудованием для отправки запросов на сервер RADIUS. Если адрес источника не указан, как адрес источника для отправки сообщений будет рассматриваться адрес интерфейса.

Идентификатор NAS (NAS-Identifier)
Настраиваемый диапазон: 0 ~ 253 символов
Функция: настройка идентификатора, используемого оборудованием для отправки сообщений на сервер RADIUS.

2. Настройка сервера RADIUS.

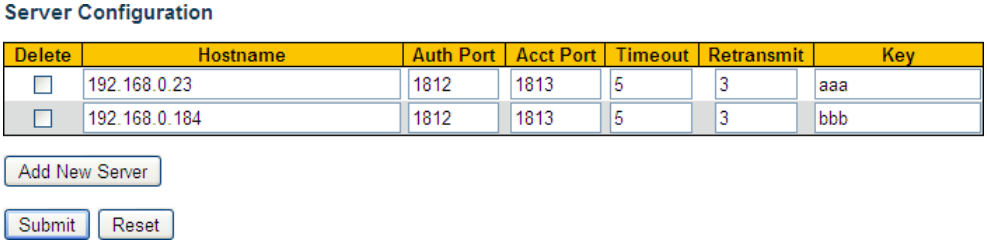


Рис. 136. Настройка сервера RADIUS

Имя хоста (Hostname)
Функция: настройка IP-адреса или имени хоста сервера RADIUS. Максимально может быть настроено 5 серверов RADIUS.
Порт аутентификации (Auth Port)
Настраиваемый диапазон (сек.): 0 ~ 65535.
Значение по умолчанию: 1812.
Функция: настройка порта UDP сервера RADIUS для аутентификации.
Порт авторизации (Acct Port)
Настраиваемый диапазон (сек.): 0 ~ 65535.
Значение по умолчанию: 1813.
Функция: настройка порта UDP сервера RADIUS для авторизации. Поскольку RADIUS использует разные порты UDP для приема и отправки сообщений при аутентификации и авторизации, настроить разные номера портов.
Таймаут (Timeout)
Настраиваемый диапазон (сек.): 1 ~ 1000 сек.
Функция: настройка времени таймаута для ответа от сервера RADIUS. Если устройство не получит ответа от сервера RADIUS после указанного времени, устройство повторно отправляет запрос на сервер RADIUS.
Количество повторов (Retransmit)
Настраиваемый диапазон (сек.): 1 ~ 1000.
Функция: настройка максимального количества попыток повторной передачи запросов на сервер RADIUS. Если устройство по-прежнему не получает ответных пакетов от сервера RADIUS после максимального количества попыток повторной передачи, аутентификация не выполняется, и устройство считает, что сервер RADIUS не рабочий.
Ключ шифрования (Key)
Настраиваемый диапазон: 0 ~ 63 символов
Функция: настройка значения ключа шифрования для повышения безопасности связи между клиентом и сервером RADIUS. Для проверки достоверности передаваемых данных, два устройства должны иметь один и тот же ключ шифрования. Таким образом, необходимо убедиться в том, что ключ клиента соответствует ключу, записанному на сервере RADIUS.

Настройки приоритета значений «Timeout», «Retransmit» и «Key» для сервера RADIUS в данном разделе выше, чем настройки в глобальной конфигурации RADIUS.

3. Просмотр статуса сервера RADIUS.

RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1	192.168.0.23	1812	Ready	1813	Ready
2	192.168.0.184	1812	Ready	1813	Ready
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Рис. 137. Отображение статуса сервера RADIUS

Нажмите соответствующий номер в первой колонке, чтобы перейти на страницу с подробной статистикой.

4. Просмотр подробной статистики сервера RADIUS.

RADIUS Authentication Statistics for Server #1

Server #1 | Auto-refresh | Refresh | Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address		192.168.0.23:1812	
State		Ready	
Round-Trip Time		0 ms	

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address		192.168.0.23:1813	
State		Ready	
Round-Trip Time		0 ms	

Рис. 138. Отображение подробной статистики сервера RADIUS

Выберите сервер и просмотрите подробную статистику соответствующего сервера.

9.10.3. Пример типовой настройки

Как показано на рис. 139, на порту 1 коммутатора включена работа протокола (стандарта) IEEE802.1X. Соответственно, пользователи могут войти в коммутатор через порт 1 после прохождения аутентификации на сервере RADIUS. IP-адрес сервера 192.168.0.23. Ключ для обмена пакетами между коммутатором и сервером: «ааа».

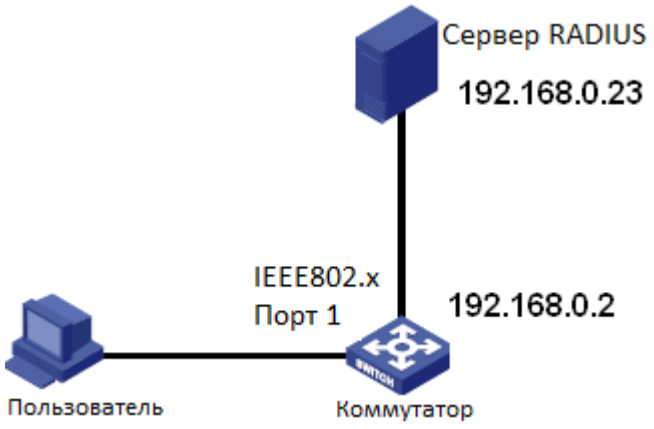


Рис. 139. Пример аутентификации RADIUS

1. Настройте IP-адрес сервера аутентификации как 192.168.0.23 и пароль как «aaa» (см. рис. 136).
2. Настройки IEEE802.1x: включите IEEE802.1X глобально. Настройте тип аутентификации как «radius», состояние администратора порта 1 как порт на основе 802.1X. Оставьте настройки по умолчанию для других параметров. Подробности см. в разделе «Конфигурация IEEE802.1X».
3. Настройте имя пользователя и пароль на сервере RADIUS как «ccc», а ключ шифрования как «aaa».
4. Установите и запустите клиентское программное обеспечение 802.1x на ПК. Введите «ccc» в качестве имени пользователя и пароля. Соответственно пользователь сможет пройти аутентификацию и получить доступ к коммутатору через порт 1.

10. Сеть (Network)

10.1. Безопасность порта

10.1.1. Введение

Режим безопасности порта ограничивает максимальное количество пользователей на порт, которые идентифицируются по MAC-адресам и идентификатором VLAN. Если для порта включено ограничение MAC-адресов, то максимальное количество пользователей на порту - это ограничение MAC-адресов. Если количество MAC-адресов на порту превышает максимальный предел, выполняется соответствующее действие.

10.1.2. Настройка через WEB-интерфейс

1. Настройка ограничения MAC-адресов для безопасности порта.

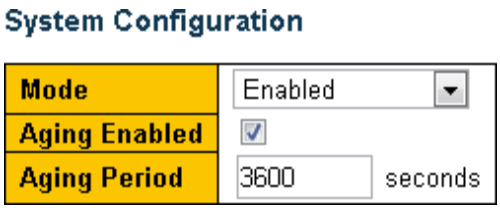


Рис. 140. Настройки системы

Режим (Mode)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение глобального режима ограничения MAC-адресов.
Функция старения (Aging Enable)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение глобальной функции старения MAC-адресов.
Период старения (Aging Period)
Настраиваемый диапазон: 10 ~ 10000000 сек.

Значение по умолчанию: 3600 сек.
Функция: MAC-адреса могут устаревать в течение данного периода.

2. Настройка ограничения MAC-адресов на порту.

Port Configuration

Port	Mode	Limit	Action	State	Reopen
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Enabled	4	None	Ready	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen

Submit Reset

Рис. 141. Настройки порта

Режим (Mode)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение режима ограничения MAC-адресов на порту.
Период старения (Aging Period)
Настраиваемый диапазон: 1 ~ 1024.
Значение по умолчанию: 4.
Функция: настройка максимального количества MAC-адресов.

Действие (Action)
Опции: None/Trap/Shutdown/Trap&Shutdown.
Значение по умолчанию: None.
Функция: если предел MAC-адресов достигнут, коммутатор может выполнить одно из следующих действий:
None: не разрешать подключение к порту больше установленного максимума MAC-адресов и не предпринимать дальнейших действий.
Trap: если порт видит MAC-адреса с ограничением + 1, то отправляется сообщение «Trap» на сервер SNMP. Если устаревание отключено, отправляется только одно сообщение «Trap» на сервер SNMP. При включенном устаревании новые сообщение «Trap» на сервер SNMP будут отправляться каждый раз при превышении лимита MAC-адресов.
Shutdown: если порт видит MAC-адреса с ограничением + 1, порт отключается. Это означает, что все безопасные MAC-адреса будут удалены из порта, а новый адрес не будет принят. Даже если соединение с портом физически отключено и затем повторно подключено (путем отсоединения кабеля), порт останется выключенным. Активировать порт можно тремя способами:
1) Перезагрузите подключенный коммутатор;

2) Отключите и снова включите «Limit Control» на порту или подключенном коммутаторе,
3) Нажмите кнопку «Reopen».
Trap&Shutdown: если порт видит MAC-адреса с ограничением + 1, будут выполнены такие действия как отправка сообщения «Trap», так и «Shutdown», описанные выше.

Состояние (State)
Опции: Disabled/Ready/Limit Reached/Shutdown.

Reopen
Функция: если порт отключен данным методом, вы можете снова включить его, нажав эту кнопку.

- Для того, чтобы управление ограничениями действовало, необходимо установить режим «Enable» как для глобального режима, так и для локального.
- Обратите внимание, что нажатие кнопки «Reopen» приводит к обновлению страницы, поэтому незавершенные изменения не будут активированы.

3. Статус безопасных портов коммутатора.

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	L--	Ready	1	4
4	---	Disabled	-	-
5	---	Disabled	-	-

Рис. 142. Статус безопасных портов коммутатора

4. Статус конкретного безопасного порта коммутатора.

Port Security Status Port 5

MAC Address	VLAN ID	State	Time of Addition	Ageing Time(s)
54-e6-fc-6a-fe-a0	1	Forwarding	1970-01-01T07:19:41+00:00	3597

Рис. 143. Статус порта

10.2. Настройка IEEE802.1X

10.2.1. Введение

Для обеспечения безопасности WLAN комитет IEEE802 LAN/WAN предложил протокол 802.1X. В качестве стандартного механизма управления доступа к портам LAN в Ethernet стандарт 802.1X обеспечивает аутентификацию. Стандарт 802.1X - это управление доступом к сети на основе портов.

Управление доступом к сети на основе портов предназначено для аутентификации и управления портами устройств при доступе к локальной сети. Если пользователь проходит аутентификацию, он может получить доступ к ресурсам в локальной сети. Если он не может пройти аутентификацию, он не сможет получить доступ к ресурсам в локальной сети.

Стандарт 802.1X имеет структуру клиент/сервер, как показано на рис. 144. Аутентификация пользователя и авторизация управления доступом на основе порта требует следующих элементов:

Рис. 144. Структура IEEE802.1X

Клиент: обычно обозначает пользовательский терминал. Когда пользователь хочет выйти в Интернет, он запускает клиентскую программу и вводит требуемые имя пользователя и пароль. Клиентская программа отправит запрос на подключение. Клиент должен поддерживать EAPOL (расширенный протокол аутентификации по локальной сети).

Устройство: означает коммутатор аутентификации в системе Ethernet. Он загружает и доставляет информацию об аутентификации пользователя, а также включает или отключает порт в зависимости от результата аутентификации.

Сервер: означает объект, который предоставляет услугу аутентификации для устройств. Он проверяет, есть ли у пользователей разрешения на использование сетевых служб в соответствии с идентификаторами (именами пользователей и паролями), отправляемыми клиентом и включает или отключает порты в соответствии с результатами аутентификации.

10.2.2. Настройка с помощью WEB-интерфейса

1. Настройка глобальных параметров IEEE802.1X

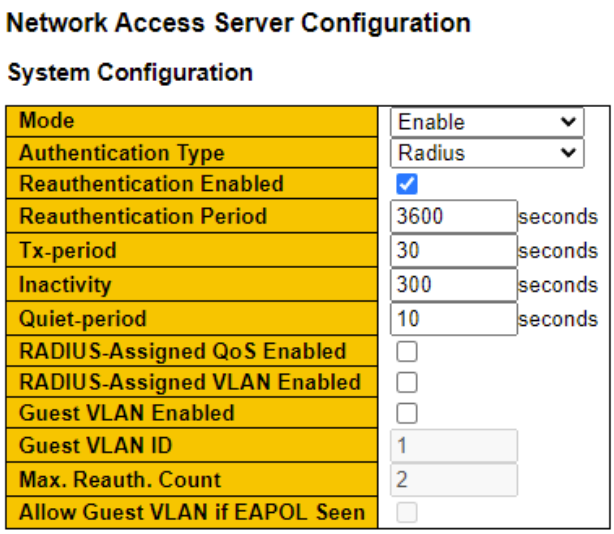


Рис. 145. Настройка глобальных параметров IEEE802.1X

Режим (Mode)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение глобального режима функции безопасности IEEE802.1x.

Включение повторной аутентификации (Reauthentication Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: настройка необходимости регулярной повторной аутентификации.

Период повторной аутентификации (Reauthentication Period)
Настраиваемый диапазон: 1 ~ 3600 сек.
Значение по умолчанию: 3600 сек.
Функция: при успешной аутентификации установите временной интервал для повторной аутентификации. Параметр «Reauthentication Period» можно настроить только при включении режима «Reauthentication Enabled».

Таймаут EAPOL (EAPOL Timeout)
Настраиваемый диапазон: 1 ~ 65535 сек.
Значение по умолчанию: 30 сек.
Функция: настройка времени таймаута для ответа от клиента. После отправки пакета с запросом «Identity EAPOL» устройство повторно отправит пакет запроса «Identity EAPOL», если оно не получит ответа от клиента после указанного времени.

Период старения (Aging Period)
Настраиваемый диапазон: 10 ~ 1000000 сек.
Значение по умолчанию: 300 сек.
Функция: настройка периода старения. Когда отключен режим «Reauthentication Enabled», временной интервал для повторной проверки подлинности составляет 2 (два) периода старения.

Таймер тишины (Quiet Timer)
Настраиваемый диапазон: 10 ~ 1000000 сек.
Значение по умолчанию: 300 сек.
Функция если аутентификация не удалась, устройство переходит в период молчания. В период молчания устройство не отвечает на запросы аутентификации от клиента.
Включение режима «RADIUS-Assigned QoS» (RADIUS-Assigned QoS Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: если этот параметр включен, то после того, как клиент проходит аутентификацию, сервер передает на устройство информацию об авторизации. Если на сервере установлен флажок «RADIUS-Assigned QoS Enabled», информация авторизации включает информацию CoS, назначенную для авторизации. Оборудование изменит значение CoS порта аутентификации клиента на основе указанного значения.
Включение режима «RADIUS-Assigned VLAN» (RADIUS-Assigned VLAN Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: если этот параметр включен, то после того, как клиент проходит аутентификацию, сервер передает на устройство информацию об авторизации. Если на сервере установлен флажок «RADIUS-Assigned VLAN Enabled», информация об авторизации включает информацию о VLAN, назначенную для авторизации. Оборудование добавит порт аутентификации клиента в назначенную VLAN.
Включение гостевого VLAN (Guest VLAN Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: если этот параметр включен, то если пользователь не прошел аутентификацию, устройство добавляет порт аутентификации клиента в гостевую VLAN. Все пользователи, которые обращаются к этому порту, имеют право доступа к ресурсам в гостевой VLAN.
Идентификатор гостевого VLAN (Guest VLAN ID)
Настраиваемый диапазон: 1 ~ 4095.
Значение по умолчанию: 1.
Функция: настройка периода идентификатора гостевого VLAN.
Счетчик максимального количества повторных аутентификаций (Max. Reauth. Count)
Настраиваемый диапазон: 1 ~ 255.
Значение по умолчанию: 2.
Функция: настройка максимального количества попыток повторной передачи для пакетов с запросом «Identity EAPO»L. Если устройство не получает ответных пакетов от клиента после максимального количества попыток повторной передачи, устройство будет считать, что аутентификация не прошла.
Разрешить гостевой VLAN, если обнаружен EAPOL (Allow Guest VLAN if EAPOL Seen)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: если этот параметр включен и если пользователь не прошел аутентификацию, устройство добавляет порт аутентификации клиента в гостевую VLAN. Если этот параметр

отключен, устройство добавляет порт в гостевую VLAN только в том случае, если этот порт не имеет записи кадра EAPOL.

- Предварительным условием при конфигурации «Guest VLAN ID», «Max. Reauth. Count», and «Allow Guest VLAN if EAPOL Seen» является включение гостевого VLAN.
- Рекомендуется отключить «RADIUS-Assigned VLAN Enabled» и «Guest VLAN ID», если тип порта аутентификации - Trunk или Hybrid.
- Значение CoS, назначенное для авторизации, не меняет и не влияет на конфигурацию порта. Однако приоритет значения CoS, назначенного для авторизации, выше, чем значение CoS, настроенное пользователем. Другими словами, то, что действительно после аутентификации, - это значение CoS, назначенное для авторизации. Если пользователю не удается пройти аутентификацию или он переходит в автономный режим, значение CoS, настроенное пользователем, вступает в силу.
- VLAN, назначенная для авторизации, или гостевая VLAN не изменяет и не влияет на конфигурацию порта. Однако VLAN, назначенная для авторизации, или гостевая VLAN имеет более высокий приоритет, чем VLAN, настроенная пользователем.

После того, как пользователь инициирует аутентификацию, и если аутентификация прошла успешно:

- если на порту включен режим **«RADIUS-Assigned VLAN»**, порт добавляется к VLAN, назначенной сервером RADIUS.
- Если на порту не включен режим **«RADIUS-Assigned VLAN»**, порт добавляется в VLAN, настроенную пользователем.

Если пользователь не может пройти аутентификацию или переходит в автономный режим:

- Если на порту включены режимы **«Guest VLAN»** и **Allow Guest VLAN if EAPOL Seen»**, порт будет добавлен к VLAN.
- Если на порту включен режим **«Guest VLAN»**, но не включен режим **«Allow Guest VLAN if EAPOL Seen»**, порт добавляется в гостевую VLAN, когда запись кадра EAPOL недоступна и добавляется в VLAN, настроенную пользователем, когда доступна запись кадра EAPOL.
- Если на порту не включен режим **«Guest VLAN»**, порт добавляется в VLAN, настроенную пользователем.

2. Настройка порта IEEE802.1X.

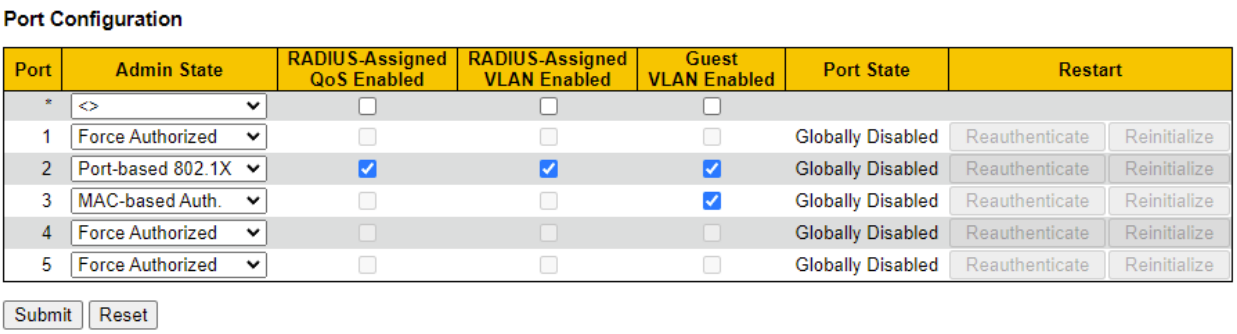


Рис. 146. Настройка порта IEEE802.1X

Порт (Port)
Опции: все порты коммутатора.
Включение гостевого VLAN (Guest VLAN Enabled)
Опции: Force Authorized/Force Unauthorized/Port-based 802.1X/MAC-based Auth.
Значение по умолчанию: Force Authorized.
Функция: выбор режима аутентификации.
Описание: «Force Authorized» означает, что порт всегда находится в авторизованном состоянии и позволяет пользователям получать доступ к сетевым ресурсам без аутентификации. «Force Unauthorized» означает, что порт всегда находится в неавторизованном состоянии и не позволяет пользователям проводить аутентификацию, а коммутатор не предоставляет услуги аутентификации клиентам, которые получают доступ к коммутатору с этого порта. Проверка подлинности на основе MAC указывает, что пользователи, использующие порт, должны быть соответственно аутентифицированы. «Port-based 802.1X» означает, что пользователи проходят аутентификацию на основе порта. После того, как первый пользователь, использующий порт, пройдет аутентификацию, все остальные пользователи, использующие порт, не нуждаются в аутентификации. Однако, если первый пользователь находится в автономном режиме, порт отключен, и все другие пользователи, использующие порт, не могут использовать сеть.
Включение режима «RADIUS-Assigned QoS» (RADIUS-Assigned QoS Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение режима «RADIUS-Assigned QoS» на порту.
Включение режима « RADIUS-Assigned VLAN Enabled » (RADIUS-Assigned VLAN Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение режима «RADIUS-Assigned VLAN Enabled» на порту.
Включение гостевого VLAN (Guest VLAN Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение гостевого VLAN на порту.

Эта функция будет доступна, только если режимы «RADIUS-Assigned QoS», «RADIUS-Assigned VLAN» и «Guest VLAN» будут включены при настройке глобальных параметров.

Включение гостевого VLAN (Guest VLAN Enabled)
Опции: Globally Disabled, Authorized, Unauthorized, Link Down, x Auth/y Unauth
Функция: отображение статуса порта.
Описание: «Globally Disabled» означает, что режим IEEE802.1X отключен глобально. «Authorized» означает, что пользователь, подключенный к порту, проходит аутентификацию; «Unauthorized» означает, что пользователь, подключенный к порту, не может пройти аутентификацию; «Link Down» означает, что порт отключен; «x Auth / y Unauth» указывает, что «X» пользователей авторизованы, а «Y» пользователей не авторизованы, если режим аутентификации порта основывается на MAC-адресах.
Если режим аутентификации порта - это аутентификация на основе MAC-адресов или 802.1X, вы можете нажать кнопку <Reauthenticate>/<Reinitialize> для повторной аутентификации. Во время повторной аутентификации состояние порта меняется на «Unauthorized».

3. Просмотр настроек IEEE802.1X

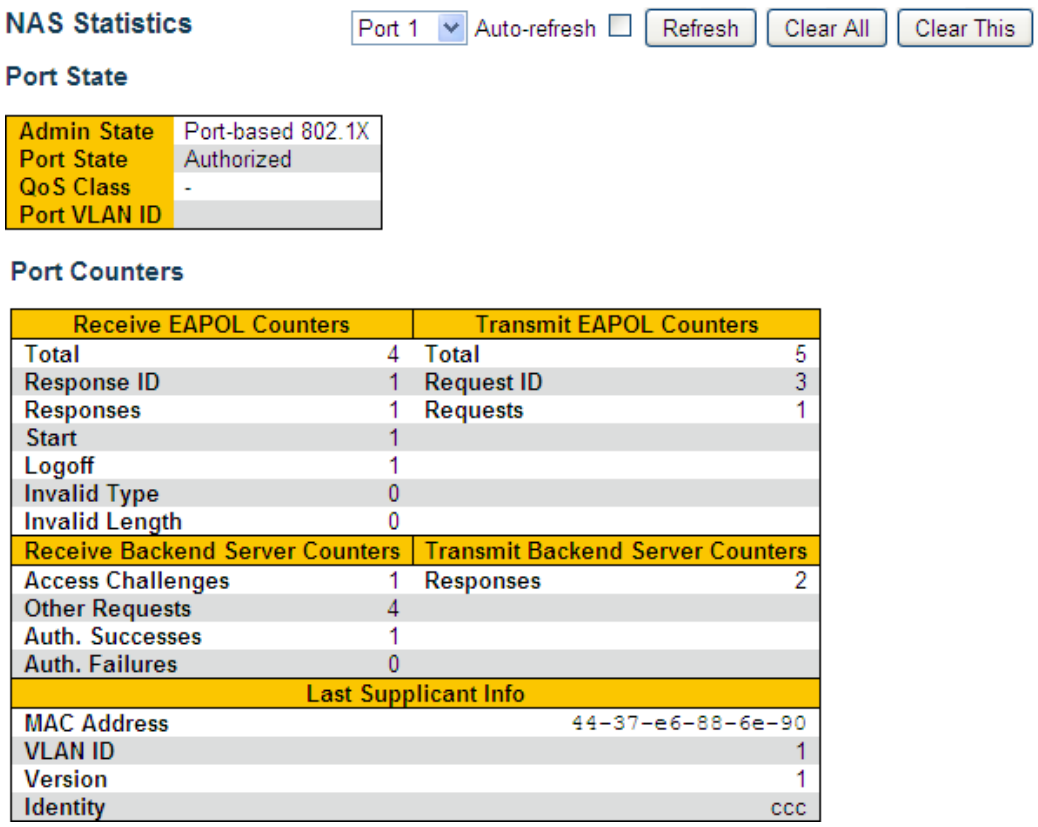
Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Port-based 802.1X	Link Down			-	
2	Force Authorized	Link Down			-	
3	MAC-based Auth.	Link Down			-	
4	Force Authorized	Authorized			-	
5	Force Authorized	Link Down			-	

Рис. 147. Отображение настроек IEEE802.1X

Нажмите <Port> для отображения статистики IEEE802.1X.

4. Просмотр статистики IEEE802.1X.



NAS Statistics Port 1 Auto-refresh Refresh Clear All Clear This

Port State

Admin State	Port-based 802.1X
Port State	Authorized
QoS Class	-
Port VLAN ID	

Port Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	4	Total	5
Response ID	1	Request ID	3
Responses	1	Requests	1
Start	1		
Logoff	1		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		**Transmit Backend Server Counters**	
Access Challenges	1	Responses	2
Other Requests	4		
Auth. Successes	1		
Auth. Failures	0		
Last Supplicant Info			
MAC Address		44-37-e6-88-6e-90	
VLAN ID		1	
Version		1	
Identity		ccc	

Рис. 148. Отображение статистики IEEE802.1X

Выберите порт и просмотрите статистику IEEE802.1X для выбранного порта.

10.2.3. Пример типовой настройки

Как показано на рис. 149, клиент подключен к порту 1 коммутатора. Включите IEEE802.1x на порту 1 и выберите режим аутентификации «Port-based 802.1X». Имя пользователя и пароль удаленной аутентификации – «ddd».

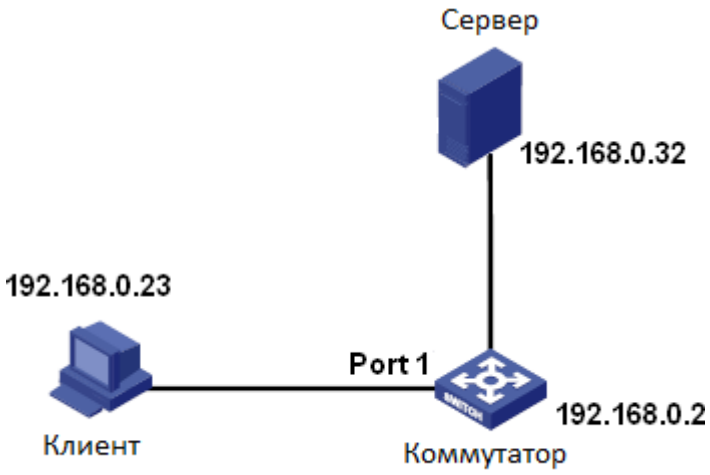


Рис. 149. Пример настройки IEEE802.1X

Вы можете обратиться к типичному примеру конфигурации в п. 9.10 «Конфигурация RADIUS».

10.3. Настройка ACL

10.3.1. Введение

С развитием сетевых технологий вопросы безопасности становятся все более заметными, требуя современных механизмов контроля доступа. С помощью функции ACL (Access Control List, Список контроля доступа) коммутатор сопоставляет пакеты со списком, который сформирован для реализации контроля доступа.

10.3.2. Реализация

Данная серия коммутаторов фильтрует пакеты в соответствии с согласованным ACL (списком доступа). Каждая запись состоит из нескольких условий в логическом отношении «И». Записи ACL независимы друг от друга.
Коммутатор сравнивает пакет с записями ACL в порядке возрастания идентификаторов записей. Как только совпадение найдено, выполняется действие, и дальнейшее сравнение не проводится.

10.3.3. Настройка с помощью WEB-интерфейса

1. Настройка портов ACL.

Конфигурация порта ACL определяет режим обработки пакетов, полученных портом, которые не соответствуют ни одной записи ACL.

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	1	Disabled / Port 1 / Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	1	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	1	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	1	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	1038
4	0	Permit	Disabled	Disabled	1	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	701
5	0	Permit	Disabled	Disabled	1	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0

Submit Reset

Рис. 150. Настройка портов ACL

Идентификатор политики (Policy ID)
Настраиваемый диапазон: 0 ~ 255.
Значение по умолчанию: 0.
Функция: настройка идентификатора политики для порта.
Действие (Action)
Опции: Deny/Permit (Запретить/Разрешить).
Значение по умолчанию: Permit (Разрешить).
Функция: настройка действия по отношению к пакету, который не соответствует ни одной записи ACL. Deny: пакеты, не соответствующие какой-либо записи, будут отклонены. Permit: пакеты, не соответствующие какой-либо записи, будут перенаправлены.
Идентификатор ограничителя скорости (Rate Limiter ID)
Настраиваемый диапазон: Disabled (Выключено)/1~16.
Значение по умолчанию: Disabled (Выключено).
Функция: выключение функции ограничения скорости и выбор идентификатора ограничителя скорости.
Идентификатор политики EVC (EVC Policer ID)
Настраиваемый диапазон: 1 ~ 256.
Значение по умолчанию: 1.
Функция: после включения политики EVC настройте идентификатор политики EVC порта.


Ограничение скорости порта и политика EVC не могут быть включены одновременно.

Функция «Port Redirect» (Port Redirect)
Опции: Disabled (Выключено) / any port (любой порт).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и отключение функции «Port Redirect». После включения этой функции пакеты, не соответствующие какой-либо записи ACL, будут перенаправлены на указанный порт.


«Port Redirect» можно включить, только если для параметра «Action» задано значение «Deny».

Функция «Mirror» (Mirror, Зеркало)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и отключение функции «Mirror» (зеркала порта). После включения этой функции пакеты, не соответствующие какой-либо записи ACL, будут перенаправлены как на порт назначения, так и на порт назначения «Mirror».


Предварительным условием для включения зеркалирования портов ACL является наличие порта назначения зеркалирования.

Функция «Logging» (Logging, Регистрация)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и отключение функции «Logging» (регистрации порта). Enabled (Включено): если порт получает пакет, не соответствующий ни одной записи ACL, пакет

записывается в системный журнал. Disable (Выключено): если порт получает пакет, не соответствующий одной из записей ACL, пакет не записывается в системный журнал.

Функция «Shutdown» (Shutdown, Отключение)

Опции: Enable/Disable (Включено/Выключено).

Значение по умолчанию: Disable (Выключено).

Функция: включение и отключение порта. Enabled (Включено): если порт получает пакет, не соответствующий ни одной записи ACL, порт отключается. Disable (Выключено): если порт получает пакет, не соответствующий записи ACL, порт не отключается.

Счетчик (Counter)

Функция: отображение количества пакетов, не совпадающих ни с одной записью ACL.

2. Настройка ограничителя скорости ACL.

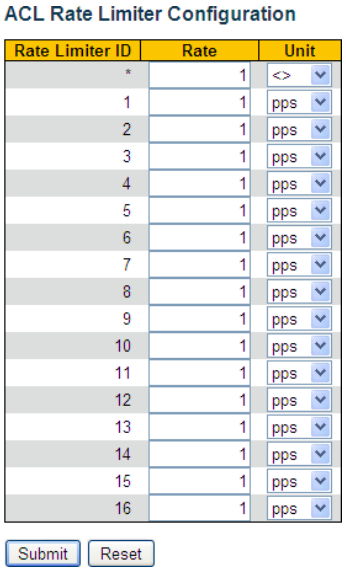


Рис. 151. Настройка ограничителя скорости ACL

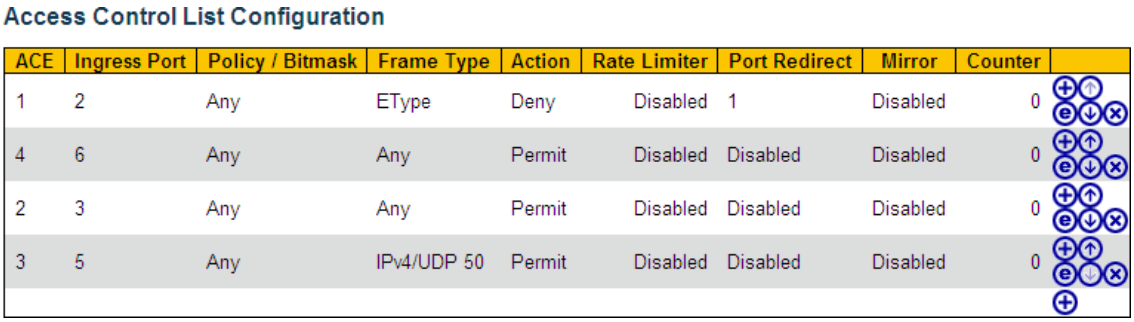
Ограничение скорости (Rate Unit)

Настраиваемый диапазон: 0~3276700 Пак/с / 0~1000000 Кбит/с (с шагом 100).

Значение по умолчанию: 1 Пак/с.

Функция: настройка ограничения скорости согласно соответствующего идентификатора.

3. Настройка записей ACL.



Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	2	Any	EType	Deny	Disabled	1	Disabled	0	
4	6	Any	Any	Permit	Disabled	Disabled	Disabled	0	
2	3	Any	Any	Permit	Disabled	Disabled	Disabled	0	
3	5	Any	IPv4/UDP 50	Permit	Disabled	Disabled	Disabled	0	

Рис. 152. Настройка записей ACL

Когда имеется несколько записей ACL, устройство сравнивает пакет с записями ACL одну за другой (сверху вниз). Как только совпадение найдено, выполняется действие, и дальнейшее сравнение не проводится.
Нажмите <⊕>, чтобы добавить новую запись ACL; нажмите <ⓔ>, чтобы отредактировать запись ACL; нажмите <⊗>, чтобы удалить запись ACL; нажмите <⊙>, чтобы переместить текущую запись вверх; нажмите <⊙>, чтобы переместить текущую запись вниз.
ACE - это идентификатор записи ACL, которая нумеруется в зависимости от времени создания записи.

4. Настройка параметров записей ACL.
   4.1. Настройка параметров записей.

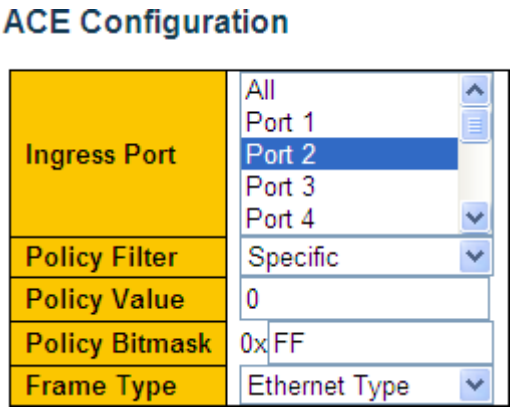


Рис. 153. Настройка параметров записей ACL

Входящий порт (Ingress Port)
Опции: All/any port (Все порты/Любой порт).
Значение по умолчанию: All (Все порты).
Функция: выбор порта, на котором действует запись управления доступом (ACE).
Фильтр политик (Policy Filter)
Опции: Any/Specific (Любой/Определенный).
Значение по умолчанию: Any (Любой).

Функция: настройка условия «ACE -> Идентификатор политик». Если для него установлено значение «Specific», необходимо установить значения «Policy value» и «Policy bitmask». Когда «Policy value» пакета, полученного входным портом, соответствует настройкам этого параметра, условие считается выполненным.

Значение политик (Policy Value)

Настраиваемый диапазон: 0 ~ 255.

Функция: настройка значения «Policy value».

Битовая маска политик (Policy Bitmask)

Настраиваемый диапазон: 0x0 ~ 0xFF.

Функция: настройка битовой маски политик. Значение политик и битовая маска политик используются для сопоставления при их фильтрации. Битовая маска политик преобразуется в двоичные цифры и затем выравнивается по правому краю со значением политики (в двоичном режиме). Значение «1» означает то же самое значение, а значение «0» означает, что разрешено любое значение.

Тип фрейма (Frame Type)

Опции Any/Ethernet Type/IPv4.

Значение по умолчанию: Any.

Функция: настройка условия «Состояние -> Тип пакета». Когда тип пакета, полученного входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

4.2. Настройка параметров VLAN.

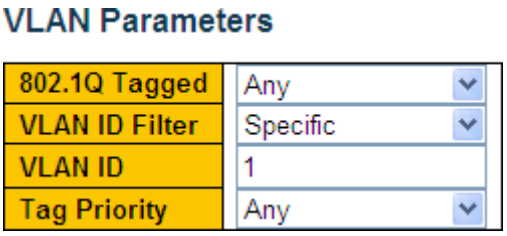


Рис. 154. Настройка параметров VLAN

Тегирование 802.1Q (802.1Q Tagged)

Опции: Any/Disabled/Enabled (Любой/Выключено/Включено).

Значение по умолчанию: Any.

Функция: настройка условия «Состояние -> Тег 802.1Q». Значение «Disabled» указывает на пакеты без тегов, а значение «Enabled» указывает на пакеты с тегами. Когда пакет, полученный входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

Фильтр идентификатора VLAN (VLAN ID Filter)

Опции: Any/Specific (1 ~ 4095).

Значение по умолчанию: Any.

Функция: настройка условия «Состояние -> VID». Если установлена опция «Specific», необходимо ввести значение VID. Когда VID в пакете, полученном входящим портом,

соответствует настройкам этого параметра, условие выполняется успешно. Если для 802.1Q Tagged установлено значение «Выключено» (Disabled), для этого параметра необходимо установить значение Any.

Приоритет тега (Tag Priority)

Опции: Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7.

Значение по умолчанию: Any.

Функция: настройка условия «Состояние -> Приоритет тега». Когда приоритет пакета, полученного входящим портом, соответствует настройкам этого параметра, условие выполняется успешно. Если для 802.1Q Tagged установлено значение «Выключено» (Disabled), для этого параметра необходимо установить значение Any.

4.3. Настройка параметров типа кадра.

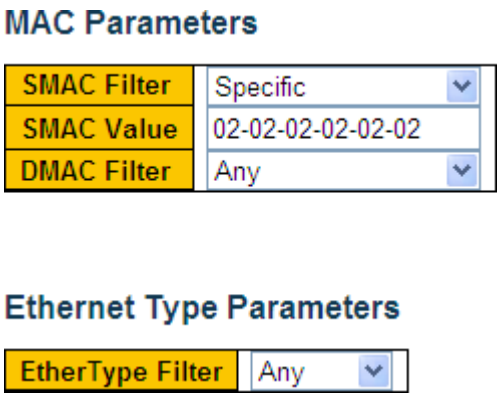


Рис. 155. Настройка параметров типа кадра

Фильтр SMAC (SMAC Filter)

Опции: Any/Specific (Любой/Определенный).

Значение по умолчанию: Any (Любой).

Функция: настройка условия «Состояние -> MAC-адрес источника». Если для него установлено значение «Specific», необходимо указать MAC-адрес источника. Если MAC-адрес источника в пакете, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

Фильтр DMAC (DMAC Filter)

Опции: Any/UC/MC/BC/Specific.

Значение по умолчанию: Any.

Функция: настройка условия «Состояние -> MAC-адрес назначения». Если для него установлено значение «Specific», необходимо указать MAC-адрес назначения. Если MAC-адрес источника в пакете, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

Фильтр типа кадра Ethernet (EtherType Filter)

Опции: Any/Specific (0x600~0xFFFF, exclude 0x800(IPv4), 0x806(ARP), 0x86DD(IPv6)).

Значение по умолчанию: Any.

Функция: настройка условия «Состояние -> Тип кадра Ethernet». Если для него установлено значение «Specific», необходимо указать тип кадра Ethernet. Если пакет Ethernet, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

4.4. Настройка параметров кадра IPv4.

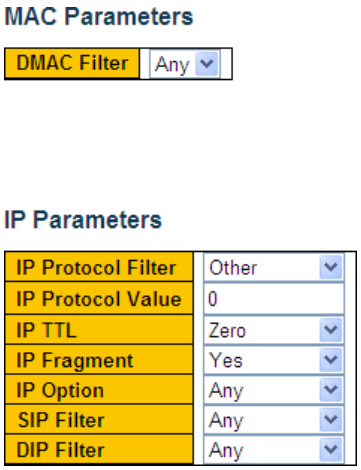


Рис. 156. Настройка параметров кадра IPv4

Фильтр DMAC (DMAC Filter)
Опции: Any/UC/MC/BC.
Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> MAC-адрес назначения». Если MAC-адрес назначения в пакете, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.
Фильтр протокола IP (IP Protocol Filter)
Опции: Any/ ICMP/ UDP/ TCP/ Other (0 ~ 255).
Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> Тип протокола пакета IPv4». Если значение установлено как ICMP, UDP или TCP, необходимо настроить соответствующие параметры. Если установлено значение «Other», необходимо установить идентификатор протокола. Когда тип протокола в пакете IPv4, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.
Поле TTL в пакетах IP (IP TTL)
Опции: Any/Non-zero/Zero.
Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> Поле TTL в пакетах IP». Значение «Non-zero» означает, что условие будет выполнено, если TTL IP в пакете IPv4 больше нуля, а значение «Zero» означает, что условие не выполняется, если TTL IP в пакете IPv4 больше нуля.
Фрагмент IP (IP Fragment)
Опции: Any/Yes/No.

Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> Фрагмент IP». Если IP-фрагмент в пакете IPv4, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

Опции IP (IP Option)
Опции: Any/Yes/No.
Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> Опции IP». Если опции IP в пакете IPv4, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

Фильтр SIP (SIP Filter)
Опции: Any/Host/Network.
Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> IP-адрес источника». Если установлено значение «Host», необходимо установить IP-адрес. Если установлено значение «Network», необходимо установить IP-адрес и маску подсети. Если IP-адрес источника в пакете IPv4, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

Фильтр DIP (DIP Filter)
Опции: Any/Host/Network.
Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> IP-адрес назначения». Если установлено значение «Host», необходимо установить IP-адрес. Если установлено значение «Network», необходимо установить IP-адрес и маску подсети. Если IP-адрес назначения в пакете IPv4, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

4.5. Настройка параметров ICMP.

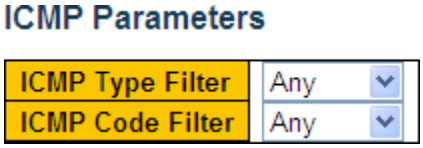


Рис. 157. Настройка параметров ICMP

Тип фильтра ICMP (ICMP Type Filter)
Опции: Any/Specific (0 ~ 255).
Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> Тип ICMP». Если установлено значение «Specific», необходимо указать тип ICMP. Если тип ICMP в пакете IPv4, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

Код фильтра ICMP (ICMP Code Filter)
Опции: Any/Specific (0 ~ 255).
Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> Код ICMP». Если установлено значение «Specific», необходимо указать код ICMP. Если код ICMP в пакете IPv4, полученном входящим портом, соответствует настройкам этого параметра, условие считается выполненным.

4.6. Настройка параметров UDP.

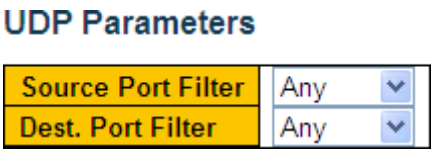


Рис. 158. Настройка параметров UDP

Фильтр порта источника/Фильтр порта назначения (Source Port Filter/ Dest. Port Filter)
Опции: Any/Specific (0 ~ 65535)/Range (0 ~ 65535).
Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> Идентификатор порта источника и идентификатор порта назначения UDP». Если установлено значение «Specific», необходимо указать идентификатор порта. Если установлено значение «Range», необходимо указать диапазон идентификаторов портов. Если идентификаторы портов UDP в пакете IPv4, полученном входящим портом, соответствуют настройкам параметров, условие считается выполненным.

4.7. Настройка параметров TCP.

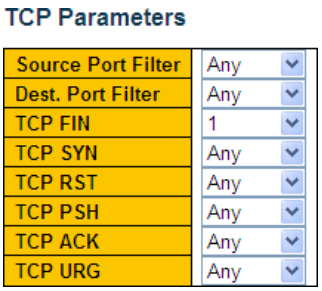


Рис. 159. Настройка параметров TCP

Фильтр порта источника/Фильтр порта назначения (Source Port Filter/ Dest. Port Filter)
Опции: Any/Specific (0 ~ 65535)/Range (0 ~ 65535).
Значение по умолчанию: Any.
Функция: настройка условия «Состояние -> Идентификатор порта источника и идентификатор порта назначения TCP». Если установлено значение «Specific», необходимо указать идентификатор порта. Если установлено значение «Range», необходимо указать диапазон идентификаторов портов. Если идентификаторы портов TCP

в пакете IPv4, полученном входящим портом, соответствуют настройкам параметров, условие считается выполненным.

TCP FIN/SYN/RST/PSH/ACK/URG

Опции: Any/1/0.

Значение по умолчанию: Any.

Функция: настройка условия «Состояние -> поля управления TCP». Если поля управления TCP в пакете IPv4, полученном входным портом, соответствуют настройкам параметров, условие считается выполненным.

4.8. Настройка действий записей ACL.

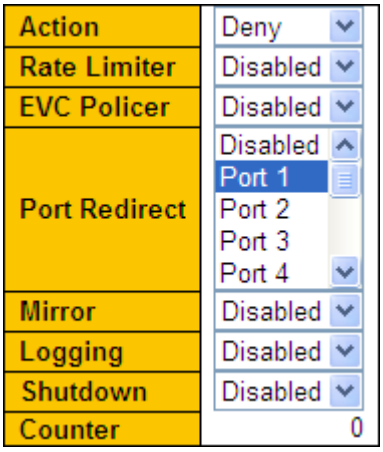


Рис. 160. Настройка действий записей ACL

Действие (Action)

Опции: Deny/Permit/Filter (Запретить/Разрешить/Фильтровать).

Значение по умолчанию: Permit (Разрешить).

Функция: настройка режима входящего порта для обработки пакета, соответствующего ACE. Значение «Deny» указывает на отказ от пакета, значение «Permit» указывает на пересылку пакета, а значение «Filter» указывает на фильтрацию пакета и необходимость выбора порта фильтрации.

Ограничитель скорости (Rate Limiter)

Настраиваемый диапазон: Disabled (Выключено)/1~16.

Значение по умолчанию: Disabled (Выключено).

Функция: выключение функции ограничения скорости и выбор идентификатора ограничителя скорости.

Политика EVC (EVC Policer)

Опции: Enable/Disable (Включено/Выключено).

Значение по умолчанию: Disable (Выключено).

Функция: включение и выключение на порту политики EVC.

Идентификатор политики EVC (EVC Policer ID)

Настраиваемый диапазон: 1 ~ 256.

Значение по умолчанию: 1.

Функция: после включения политики EVC настройте идентификатор политики EVC порта.

Ограничение скорости порта и политика EVC не могут быть включены одновременно.

Функция «Port Redirect» (Port Redirect)

Опции: Disabled (Выключено) / any port (любой порт).

Значение по умолчанию: Disabled (Выключено).

Функция: включение и отключение функции «Port Redirect». После включения этой функции пакеты, соответствующие любой записи, будут перенаправлены на указанный порт.

«Port Redirect» можно включить, только если для параметра «Action» задано значение «Deny».

Функция «Mirror» (Mirror, Зеркало)

Опции: Enable/Disable (Включено/Выключено).

Значение по умолчанию: Disable (Выключено).

Функция: включение и отключение функции «Mirror» (зеркала порта). После включения этой функции пакеты, соответствующие любой записи, будут перенаправлены как на порт назначения, так и на порт назначения «Mirror».

Предварительным условием для включения зеркалирования портов ACL является наличие порта назначения зеркалирования.

Функция «Logging» (Logging, Регистрация)

Опции: Enable/Disable (Включено/Выключено).

Значение по умолчанию: Disable (Выключено).

Функция: включение и отключение функции «Logging» (регистрации порта). Enabled (Включено): если порт получает пакет, соответствующий любой записи ACL, пакет записывается в системный журнал. Disable (Выключено): если порт получает пакет, соответствующий всем записям ACL, пакет не записывается в системный журнал.

Функция «Shutdown» (Shutdown, Отключение)

Опции: Enable/Disable (Включено/Выключено).

Значение по умолчанию: Disable (Выключено).

Функция: включение и отключение порта. Enabled (Включено): если порт получает пакет, соответствующий любой записи ACL, порт отключается. Disable (Выключено): если порт получает пакет, соответствующий всем записям ACL, порт не отключается.

Счетчик (Counter)

Функция: отображение количества пакетов, соответствующих ACE, которые получает каждый порт.

4.9. Просмотр записей ACL.

ACL Status

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
rp_mirror_cpu	1	EType	Filter	Disabled	Enabled	Yes	0	No
devSmacDrop	1	EType	Deny	Disabled	Disabled	No	0	No
bootp	1	IPv4/UDP 67-68	Filter	Disabled	Enabled	Yes	298	No
arp	1	ARP	Filter	Disabled	Enabled	Yes	199870	No
static	1	EType	Deny	Disabled	Disabled	No	0	No
static	4	Any	Permit	Disabled	Disabled	No	0	No
static	2	Any	Permit	Disabled	Disabled	No	0	No
static	3	IPv4/UDP 50	Permit	Disabled	Disabled	No	0	No
static	5	EType	Permit	Disabled	Disabled	No	0	No
static	6	IPv4/Other 0	Permit	Disabled	Disabled	No	0	No

Рис. 161. Отображение записей ACL

Конфликт (Conflict)
Опции: No/Yes (Нет/Да).
Функция: отображение статуса конфликтов записей ACL. Если ресурсов для создания записей ACL недостаточно, статус «Conflict» устанавливается в состояние «Yes» для этой записи. В противном случае для этой записи устанавливается значение «No».

10.3.4. Пример типовой настройки

Подключитесь к порту 2 коммутатора. Настройте порт для приема пакетов только с MAC-адреса источника 02-02-02-02-02-02 и пересылайте пакеты через порт 1.
Шаги настройки:
1. Настройте Действие порта на «Deny» (см. рис. 150).
2. Настройте запись ACL, настройте 2 порт как входящий, тип кадра как Ethernet (см. рис. 153).
3. Установите фильтр SMAC на 02-02-02-02-02-02 (см. рис. 155).
4. Настройте Действие записи ACL как «Deny», установите функцию «Port redirect» для порта 1 (см. рис. 160).
5. Оставьте все остальные параметры по умолчанию или пустыми.

11. Агрегация портов (Port Aggregation)

11.1. Статическая агрегация

11.1.1. Введение

Функция агрегации портов предназначена для привязки группы физических портов с одинаковой конфигурацией к логическому порту для увеличения пропускной способности и скорости передачи. Порты-участники в одной группе совместно используют трафик и служат в качестве динамических резервных копий друг для друга, повышая надежность соединения.
Группа портов - это группа физических портов имеющих одинаковую конфигурацию. Только физические порты могут участвовать в агрегации каналов. Если физические порты в группе портов соответствуют определенным условиям, они обеспечивают агрегацию

каналов, которые становятся независимыми логическими портами, тем самым увеличивая пропускную способность сети и обеспечивая резервирование.

11.1.2. Реализация

Как показано на рис.162, три порта коммутатора А объединены (агрегированы) в группу (канал агрегации). Пропускная способность канала агрегации является общей пропускной способностью трех портов.

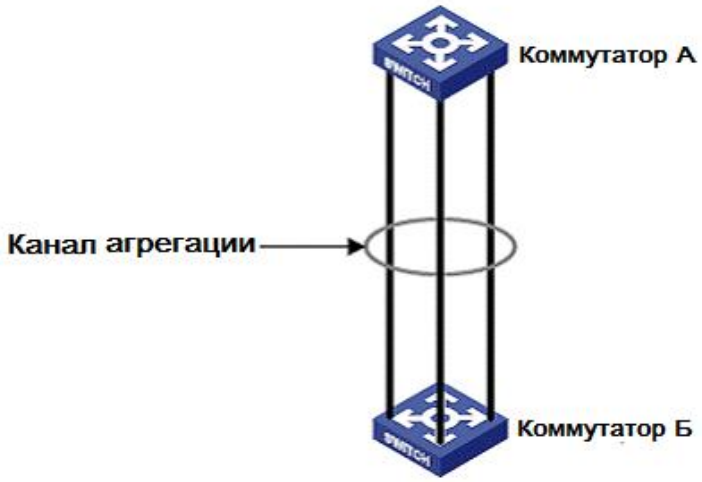


Рис. 162. Группа каналов агрегации

Когда коммутатор А передает данные для коммутатора В через канал агрегации, коммутатор А будет распределять потоки данных в соответствии с определенным алгоритмом, при этом только один порт будет выбран для передачи данных. Если произойдет сбой на одном из портов канала агрегации, данные передаваемые этим портом в соответствии с определенным алгоритмом будут перераспределены на другой нормально работающий порт.

- Порт можно добавить только в одну группу портов.
- Только полнодуплексные порты могут присоединяться к агрегации.
- Для порта, включенного в канал агрегации, нельзя включить LACP, а порт с включенным LACP нельзя добавить в канал агрегации.
- Порт, включенный в канал агрегации и порт, являющийся портом резервирования, исключают друг друга. Порт, включенный в канал агрегации, не может быть настроен как резервный порт, а резервный порт не может быть добавлен в канал агрегации.
- Под резервным портом в этом документе понимается кольцевой порт Sy2-Ring, резервный порт Sy2-Ring, кольцевой порт Sy2-RP, резервный порт Sy2-RP, порт RSTP и порт MSTP.

11.1.3. Настройка с помощью WEB-интерфейса

1. Настройка режима распределения нагрузки.

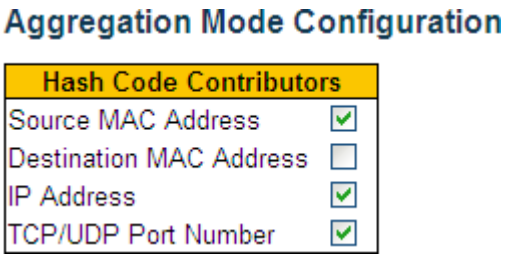


Рис. 163. Настройка режима распределения нагрузки

Режим распределения нагрузки (Hash Code Contributors)
Опции: Source MAC Address/Destination MAC Address/IP Address/ TCP/UDP Port Number.
Значение по умолчанию: Source MAC Address/IP Address/ TCP/UDP Port Number.
Функция: настройка режима распределения нагрузки.
Описание: MAC-адрес источника означает распределение нагрузки на основе MAC-адреса источника. MAC-адрес назначения означает распределение нагрузки на основе MAC-адреса назначения. IP-адрес означает распределение нагрузки на основе IP-адреса. Номер порта TCP/UDP означает распределение нагрузки на основе номера порта TCP/UDP.

2. Настройка портов для канала агрегации.

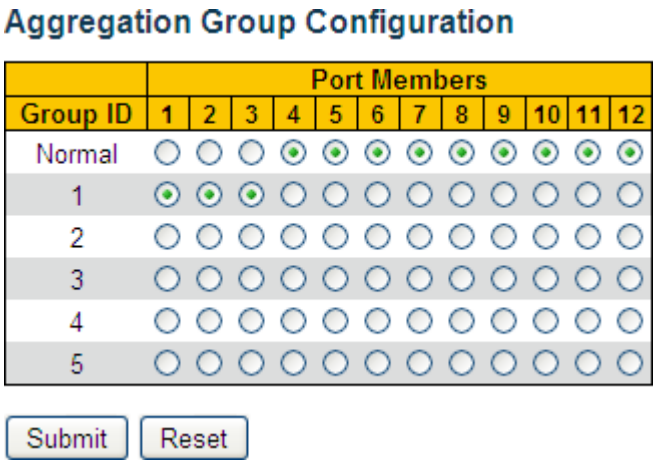


Рис. 164. Настройка портов для канала агрегации

Порты-участники группы (Port Member)
Функция: выбор портов-участников группы канала агрегации.
Описание: Все порты-участники в одной группе агрегации имеют одинаковую конфигурацию. Количество транковых групп зависит от количества портов коммутатора. Каждая группа может содержать максимум 8 портов.

11.1.4. Пример типовой настройки

Добавьте три порта (порт 1, 2 и 3) коммутатора A в группу портов (канал агрегации) «1» и три порта (порт 1, 2 и 3) коммутатора B в группу портов (канал агрегации) «1» (см. рис. 162), чтобы сформировать канал агрегации и реализовать распределение нагрузки между портами. Для соединения этих портов используйте стандартные сетевые кабели. (Предполагается, что три порта на коммутаторе A и B имеют одинаковые параметры соответственно).

Настройки коммутатора:

1. Добавьте порт 1, 2 и 3 коммутатора A в группу портов «1» (см. рис. 164).
2. Добавьте порт 1, 2 и 3 коммутатора B к группе портов «1» (см. рис. 164).

11.2. Протокол LACP

11.2.1. Введение

Протокол управления агрегацией каналов (LACP, Link Aggregation Control Protocol) основан на стандарте IEEE802.3ad. Он используется для обмена информацией с портом входящих соединений (peer-port) через блок данных протокола управления агрегацией каналов (LACPDU, Link Aggregation Control Protocol Data Unit), для выбора порта-участника динамической группы агрегации.

11.2.2. Реализация

Порт с включенным протоколом LACP информирует peer-port о приоритете данного LACP для локального оборудования, MAC-адреса оборудования, порта LACP, номера порта и значении ключа, отправляя сообщение LACPDU. После получения сообщения LACPDU Peer-port согласовывает с локальным портом следующее:

- сопоставляет идентификаторы оборудования на обоих концах (идентификатор оборудования = приоритет LACP оборудования + MAC-адрес оборудования). Сначала сопоставляются приоритеты LACP. Если приоритеты LACP совпадают, сопоставляются их MAC-адреса. В качестве основного (master) выбирается оборудование с наименьшим идентификатором.
- сопоставляются идентификаторы портов основного (master) оборудования (идентификатор порта = приоритет LACP порта + номер порта). Сначала сопоставляются приоритеты портов LACP. Если приоритеты портов LACP совпадают, сопоставляются номера портов. В качестве ссылочного (reference) порта выбирается порт с наименьшим идентификатором.
- если основной порт и ссылочный порт имеют одинаковые значения ключей и одинаковые конфигурации атрибутов порта в состоянии «Up», этот порт может стать портом-участником группы динамической агрегации портов.

11.2.3. Настройка через WEB-интерфейс

1. Настройка порта LACP.

LACP Port Configuration

Ports	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768

Submit Reset

Рис. 165. Настройка портов LACP

Включение LACP (LACP Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение протокола LACP на порту.

Ключ (Key)
Настраиваемый диапазон: Auto/Specific (1 ~ 65535).
Значение по умолчанию: Auto.
Функция: настройка значения ключа для порта. «Auto» означает, что значение ключа зависит от скорости порта, ключ = 1 (10 МБ), ключ = 2 (100 МБ), ключ = 3 (1000 МБ). Порты с разными значениями ключей нельзя добавить в группу агрегации.

Роль (Role)
Опции: Active/Passive (Активно/Пассивно).
Значение по умолчанию: Active (Активно).
Функция: выбор состояния роли LACP. Активный порт будет активно отправлять сообщения LACPDU на peer-port. Пассивный порт будет отправлять сообщения LACPDU на peer-port после получения сообщений LACPDU от peer-port.

Для двух подключенных портов должен быть активен хотя бы один порт; в противном случае два порта не смогут обмениваться информацией друг с другом.

Таймаут (Timeout)
Опции: Fast/Slow (Быстро/Медленно).
Значение по умолчанию: Fast (Быстро).
Функция: настройка интервала для активного порта при отправке сообщений LACPDU. «Fast» означает, что интервал равен 1 сек. «Slow» означает, что интервал равен 30 сек.

Приоритет (Prio)
Настраиваемый диапазон: 1 ~ 65535.
Значение по умолчанию: 32768.
Функция: настройка приоритета порта LACP, который используется для выбора ссылочного (reference) порта. Порт с более низким приоритетом в основном устройстве выбирается в качестве ссылочного порта.

2. Просмотр статуса LACP.

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
LLAG1	00-01-c1-01-00-02	2	32768	0d 00:00:28	1,2

Рис. 166. Отображение статуса LACP

3. Просмотр статуса порта LACP.

LACP Status

Ports	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-

Рис. 167. Отображение статуса порта LACP

LACP
Опции: Yes/No (Да/Нет).
Функция: отображение статуса порта LACP. «Yes» означает, что LACP включен и порт подключен. «No» означает, что LACP выключен или порт не работает.

4. Просмотр статистики порта LACP.

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0

Рис. 168. Отображение статистики порта LACP

11.2.4. Пример типовой настройки

Добавьте три порта (порт 1, 2 и 3) коммутатора A в группу портов (канал агрегации) «1» и три порта (порт 1, 2 и 3) коммутатора B в группу портов (канал агрегации) «1» (см. рис. 162), чтобы сформировать канал агрегации и реализовать распределение нагрузки между

портами. Для соединения этих портов используйте стандартные сетевые кабели. (Предполагается, что три порта на коммутаторе A и B имеют одинаковые параметры соответственно).

Настройки коммутатора:

1. Включите LACP на портах 1, 2 и 3 коммутатора A (см. рис. 165).
2. Включите LACP на портах 1, 2 и 3 коммутатора B (см. рис. 165).

12. Настройка функции Loop Protection

12.1. Введение

После того, как на порту будет включена функция обнаружения петель (Loop Protection), через порт будут отправляться специальные пакеты для обнаружения петель. Данная функция определяет, существуют ли петли в сети, подключенной к порту. ЦП (CPU) периодически передает на порт пакеты «Loop Protection». Если какой-либо порт коммутатора получает пакеты «Loop Protection», можно сказать, что в сети существуют петли. Перезагрузите порт, который отправляет пакеты «Loop Protection», и через некоторое время порт будет автоматически подключен и продолжит обнаружение. Интервал времени для отправки пакетов обнаружения петель и время восстановления порта можно настроить в программном обеспечении.

Функция обнаружения петель и использование протоколов резервирования Sy2-Ring/Sy2-RP/RSTP/MSTP являются взаимоисключающими. Порт с включенной функцией обнаружения петель не может быть настроен как резервный порт и обратно.

12.1.1. Настройка через WEB-интерфейс

1. Настройка функции обнаружения петель.

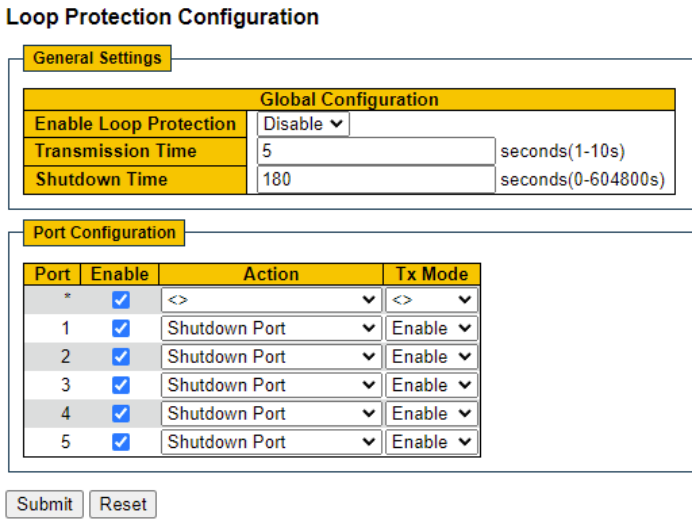


Рис. 169. Настройка функции обнаружения петель

Включение Loop Protection (Enable Loop Protection)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение глобальной функции обнаружения петель на порту.
Время передачи (Transmission Time)
Настраиваемый диапазон: 1 ~ 10 сек.
Значение по умолчанию: 5 сек.
Функция: настройка интервала времени передачи пакетов «Loop Protection».
Время перезагрузки (Shutdown Time)
Настраиваемый диапазон: 0 ~ 604800 сек.
Значение по умолчанию: 180 сек.
Функция: настройка времени восстановления порта. «0» означает, что порт не может быть подключен автоматически до перезапуска устройства.
Включение (Enable)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение функции обнаружения петель на порту.
Действие (Action)
Опции: Shutdown Port/Shutdown Port and Log/Log Only (Перезагрузка порта/Перезагрузка порта и запись логфайла/Только запись логфайла).
Значение по умолчанию: Shutdown Port (Перезагрузка порта).
Функция: выполнение действия, которое будет выполняться, когда порт обнаруживает наличие петли.
Режим Tx (Tx Mode)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение функции отправки пакетов обнаружения петель.

Порт может точно определить, существует ли петля, только после того, как функция обнаружения петель включена глобально, включены параметры на порту и включен режим Tx.

2. Просмотр статуса функции обнаружения петель.

Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	14	Down	-	2015-11-14T13:29:24+08:00
3	Shutdown	Enabled	8	Disabled	Loop	2015-11-14T13:30:55+08:00
4	Shutdown	Enabled	1	Down	-	2015-11-14T13:26:33+08:00
5	Shutdown	Enabled	0	Down	-	-

Рис. 170. Отображение статуса функции обнаружения петель

Статус функции обнаружения петель (Loop Protection Status)
Опции: --/Loop.
Функция: отображение показывает, есть ли петли в сети, в которой включена функция обнаружения петель на порту. «Loop» указывает на наличие петель, в то время как – показывает их отсутствие.

12.1.2. Пример типовой настройки

Требования к сети:
Порт 3 коммутатора подключен к внешней сети. Когда в сети есть петли, отключите порт 3, как показано на рис. 171.

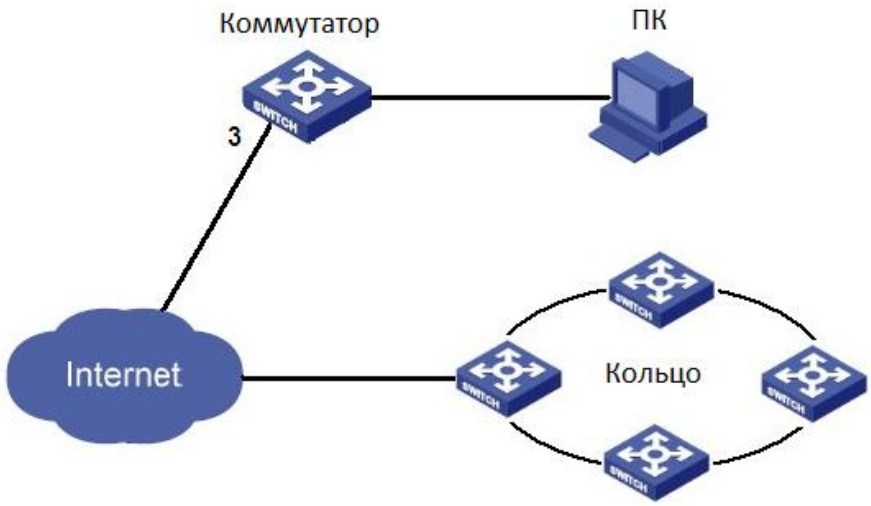


Рис. 171. Схема сети

Конфигурация:
Включите функцию обнаружения петель порта 3, как показано на рис. 169.

13. Промышленные протоколы (Industry Protocol)

13.1. Ethernet /IP

13.1.1. Введение

EtherNet/IP - это промышленный протокол прикладного уровня для приложений промышленной автоматизации. Он основан на стандартных протоколах TCP/IP и UDP/IP и использует стандартное оборудование и программное обеспечение сети Ethernet для определения и настройки протоколов прикладного уровня, а также доступа и управления устройствами промышленной автоматизации.
Реализация протокола EtherNet/IP для данной серии коммутаторов дает возможность пользователям настраивать статус порта (включен/выключен) для получения информации

об устройстве, о портах, о сигналах тревоги, информации о кольцевых протоколах Sy2-Ring, Sy2-RP и RSTP.

13.1.2. Настройка через WEB-интерфейс

1. Настройка протокола EtherNet/IP.

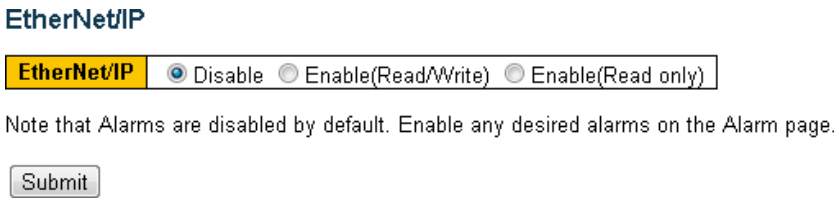


Рис. 172. Настройка протокола EtherNet/IP

Настройка EtherNet/IP (EtherNet/IP)
Опции: Disable (Выключено)/Enable(Read/Write) (Включено «Чтение/Запись»)/Enable(Read Only) (Включено «Только чтение»).
Значение по умолчанию: Disable (Выключено).
Функция: включение протокола EtherNet/IP и использование его для настройки статуса устройства.

13.2. Modbus TCP

13.2.1. Введение

Протокол Modbus TCP – это обычный протокол Modbus, основанный на стандарте Ethernet TCP/IP. Modbus - это протокол передачи сообщений прикладного уровня, в котором для связи используется Master/Slave (ведущий/ведомый). Modbus - это простой протокол для приложений клиент/сервер. Задача сервера – анализ, обработка запросов и передача ответов клиенту.
Реализация протокола ModbusTCP для данной серии коммутаторов дает возможность пользователям настраивать статус порта (включен/выключен) для получения информации об устройстве, о порте, о сигналах тревоги, информации о кольцевых протоколах Sy2-Ring, Sy2-RP и RSTP.

13.2.2. Настройка через WEB-интерфейс

1. Настройка протокола Modbus TCP.

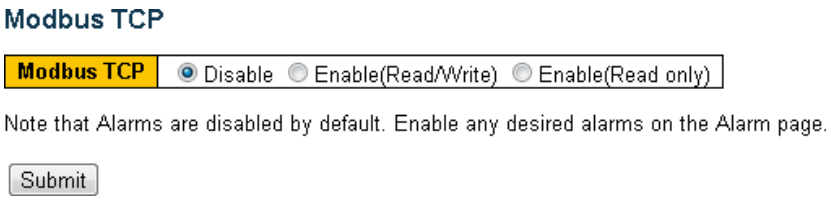


Рис. 173. Настройка протокола Modbus TCP

Настройка Modbus TCP (Modbus TCP)
Опции: Disable (Выключено)/Enable(Read/Write) (Включено «Чтение/Запись»)/Enable(Read Only) (Включено «Только чтение»).
Значение по умолчанию: Disable (Выключено).
Функция: включение протокола EtherNet/IP и использование его для настройки статуса устройства.

14. Многоадресная рассылка (Multicast)

14.1. IMGP Snooping

14.1.1. Введение

IGMP Snooping (Internet Group Management Protocol Snooping) - многоадресный протокол второго уровня, работающий на уровне канала передачи данных. Он используется для управления и настройки многоадресных групп передачи данных. Коммутаторы с поддержкой IGMP Snooping анализируют принимаемые IGMP пакеты, устанавливают соответствие между портами и MAC-адресами многоадресной рассылки и отправляют многоадресные сообщения согласно этим соответствием.
Существует три версии IGMP: IGMPv1, IGMPv2 и IGMPv3. IGMPv1 определен в RFC1112, IGMPv2 определен в RFC2236, а IGMPv3 определен в RFC3376.
IGMPv1 поддерживает два типа пакетов (пакеты отчетов и запросов) и определяет основные запросы членов группы и процесс отчетов.
IGMPv2, построенный на основе IGMPv1, обеспечивает механизм быстрого выхода для членов группы. С помощью этого механизма, когда последний участник покидает группу многоадресной рассылки, маршрутизатор получает указание провести быструю конвергенцию. По сравнению с IGMPv1, IGMPv2 поддерживает два типа пакетов запроса: общий пакет запроса и пакет запроса для конкретной группы. Коммутатор периодически отправляет общий пакет запроса для запроса членства. Когда хост покидает группу многоадресной рассылки, и после того, как коммутатор получает сообщение о выходе, коммутатор отправляет пакет запроса для конкретной группы, чтобы определить, все ли члены покинули группу многоадресной рассылки.
В IGMPv3 добавлена функция фильтрации источника хоста. Эта функция позволяет хосту указать, принимать или отклонять пакеты от некоторых определенных источников группы многоадресной рассылки.

14.1.2. Концепция

Генератор запросов (Querier): периодически отправляет IGMP запросы для проверки и обновления информации о многоадресных группах чтобы узнать активны ли они и обеспечить поддержку групповой передачи. Если в сети присутствует несколько генераторов запросов, они автоматически определяют одного (с наименьшим IP

адресом), который непосредственно и будет осуществлять запросы, остальные будут только получать и передавать IGMP запросы.
Маршрутизирующий порт (Router port): получает запросы (на IGMP-коммутаторе) от генератора. При получении IGMP ответа, коммутатор инициализирует многоадресную группу и добавляет в неё порт, на который пришёл ответ. Если настроен маршрутизирующий порт, он также добавляется. Затем коммутатор ретранслирует IGMP ответ другим устройствам через маршрутизирующий порт.
Прокси-сервер IGMP snooping (IGMP snooping proxy): данная функция настраивается на граничном устройстве, чтобы уменьшить количество пакетов с отчетами IGMP и сохранить пакеты, полученные вышестоящим (upstream) устройством, для улучшения его общей производительности. Устройство, на котором настроена функция прокси-сервера, функционирует как хост для своего вышестоящего устройства и функционирует как генератор запросов (Querier) для нисходящего (downstream) хоста.

14.1.3. Принцип работы

IGMP Snooping управляет членами многоадресных групп путём обмена пакетами между поддерживающих IGMP устройств. Данные запросы содержат следующие важные сообщения:

- пакет с общим запросом: генератор запросов периодически отправляет общие запросы (с фиксированным IP адресом назначения: 224.0.0.1) для уточнения, есть ли у многоадресной группы порты участники группы. При получении запроса, устройство, не являющееся генератором запросов, ретранслирует пакет на все свои порты.
- пакет с конкретным запросом: если устройство хочет покинуть многоадресную группу, оно отправляет пакет "IGMP leave". После получения такого пакета, генератор запросов отправляет пакет конкретного запроса (с IP адресом назначения, соответствующим IP адресу многоадресной группы) для подтверждения того, что у коммутатора остались какие-либо порты участники данной группы.
- пакет с отчетом участника группы: если устройство хочет получать определенные данные многоадресной группы, оно отправляет пакет IGMP оповещения (с IP адресом назначения, соответствующим IP адресу многоадресной группы, к которой устройство планирует присоединиться) в ответ на IGMP запрос группы.
- пакет "IGMP leave": Если устройство хочет покинут многоадресную группу, оно отправляет пакет "IGMP leave" (с фиксированным IP адресом назначения: 224.0.0.2).

14.1.4. Настройка через WEB-интерфейс

1. Включение IGMP Snooping

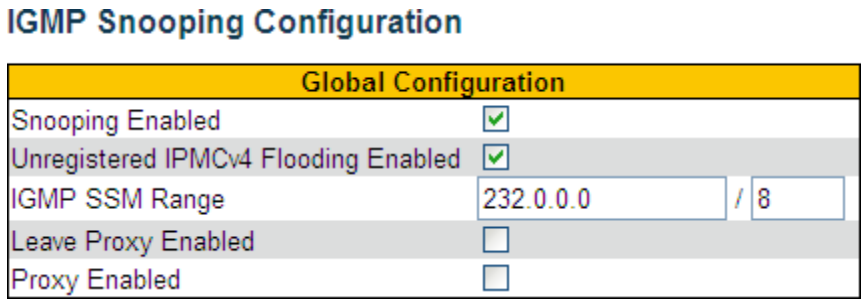


Рис. 174. Включение IMGP Snooping

Включение Snooping (Snooping Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение глобальной функции протокола IMGP Snooping.

Включение незарегистрированного IPMCv4 Flooding (Unregistered IPMCv4 Flooding Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Enable (Включено).
Функция: настройка незарегистрированного действия многоадресной рассылки. Enable: при получении незарегистрированного многоадресного пакета коммутатор транслирует пакет в рамках VLAN (все порты, кроме входящего). Disable: при получении незарегистрированного многоадресного пакета коммутатор его отбрасывает. Незарегистрированные многоадресные пакеты относятся к многоадресным пакетам без соответствующих записей пересылки на коммутаторе.

Диапазон IGMP SSM (IGMP SSM Range)
Формат: A.B.C.D/4~32.
Значение по умолчанию: 232.0.0.0/8.
Функция: только хосты и маршрутизаторы с адресом в пределах значения этого параметра могут запускать сервисную модель многоадресной рассылки IGMP, зависящей от источника (SSM), при условии, что хосты и маршрутизаторы поддерживают сервисную модель IGMP SSM. Модель службы SSM предоставляет пользователям услугу передачи с указанием для клиента источников многоадресной рассылки.

Включение функции Leave Proxy (Leave Proxy Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение функции пересылки исходящих пакетов запрашивающей стороне. Когда функция включена, исходящие пакеты не пересылаются.

Включение Proxy (Proxy Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение функции пересылки исходящих пакетов и пакетов с отчетами запрашивающей стороне. Когда функция включена, исходящие пакеты и пакеты с отчетами не пересылаются.

2. Настройка порта IGMP

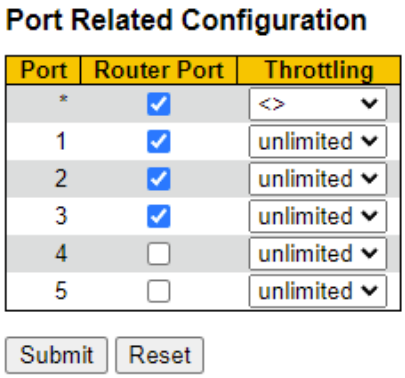


Рис. 175. Настройка порта IGMP

Маршрутизирующий порт (Router Port)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение маршрутизирующего порта.
Регулирование записей (Throttling)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение функции ограничения количества многоадресных записей, полученных портом.

3. Настройка VLAN IGMP Snooping.

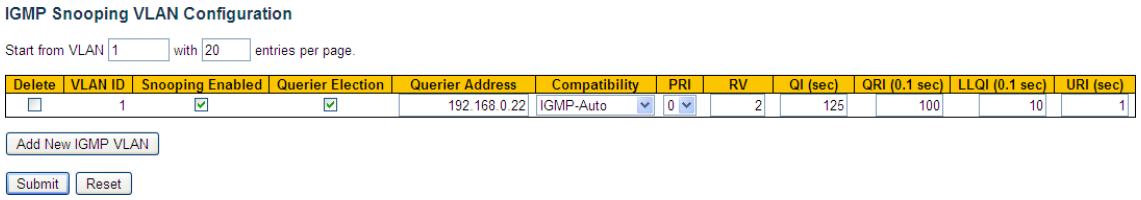


Рис. 176. Настройка VLAN IGMP Snooping

Идентификатор VLAN (VLAN ID)
Опции: все созданные идентификаторы VLAN.
Включение Snooping (Snooping Enabled)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: включение и выключение функции VLAN IMGP Snooping. Предварительным условием для включения этой функции является включение глобальной функции IGMP Snooping.
Функция запросов (Querier Election)
Опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).

Функция: включение и выключение функции запроса IGMP для выбранной VLAN. Предварительным условием для включения этой функции является включение глобальной функции IGMP Snooping и функции VLAN IGMP Snooping.
Описание: если в сети несколько генераторов запроса, в качестве запрашивающего автоматически будет выбран тот, у кого наименьший IP-адрес. Если есть только одно устройство, для которого включена функция запроса IGMP, оно будет запрашивающим.

Адрес запрашивающего (Querier Address)
Формат: A.B.C.D
Функция: настройка исходящего IP-адреса для отправки пакетов с запросом. Если адрес запрашивающей стороны не установлен, IP-адрес порта VLAN используется в качестве адреса запрашивающей стороны.

Совместимость (Compatibility)
Опции: IGMP-Auto/Forced IGMPv1/Forced IGMPv2/Forced IGMPv3.
Значение по умолчанию: IGMP-Auto.
Функция: настройка версии IGMP.

Приоритет интерфейса (PRI, Priority of Interface)
Настраиваемый диапазон: 0 ~ 7.
Значение по умолчанию: 0.
Функция: настройка приоритета управляющего пакета IGMP.

Переменная надежности (RV, Robustness Variable)
Настраиваемый диапазон: 1 ~ 255.
Значение по умолчанию: 2.
Функция: настройка параметра надежности функции запроса IGMP.
Описание: чем больше параметр, тем хуже сетевая среда. Пользователь может установить подходящий параметр надежности в соответствии с реальной сетью.

Интервал запроса (QI, Query Interval)
Настраиваемый диапазон: 1 ~ 31744 сек.
Значение по умолчанию: 125 сек.
Функция: настройка интервала отправки запроса основного пакета.

Интервал ответа на запрос (QRI, Query Response Interval)
Настраиваемый диапазон: 1 ~ 31744 (шаг: 0,1 сек.).
Значение по умолчанию: 100.
Функция: настройка максимального времени ответа на запрос основного пакета.

Интервал запроса последнего участника (LLQI, Query Response Interval)
Настраиваемый диапазон: 1 ~ 31744 (шаг: 0,1 сек.).
Значение по умолчанию: 10.
Функция: настройка максимального времени ответа на соответствующий запрос пакета.

Конфигурация QI, QRI и LLQI действительна только для запрашивающего.

Интервал для не запрашиваемого отчета (URI, Unsolicited Report Interval)
Настраиваемый диапазон: 1 ~ 31744 сек.
Значение по умолчанию: 1 сек.

Функция: настройка интервала для хоста при повторной отправке пакета с отчетом для присоединения к группе многоадресной рассылки. Нажмите <Add New IGMP VLAN>, чтобы настроить запись VLAN IGMP Snooping. Поддерживается максимум 32 записи VLAN IGMP Snooping.

4. Просмотр статуса IGMP Snooping.

IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v2	v2	ACTIVE	209	84	0	1541	140	78
2	v3	v3	ACTIVE	0	0	0	0	0	0
3	v3	v3	ACTIVE	0	0	0	0	0	0

Router Port

Port	Status
1	Both
2	Static
3	Static
4	Both
5	-

Рис. 177. Настройка VLAN IGMP Snooping

Статус маршрутизирующего порта (Router Port Status)
Опции: Both/Static/Dynamic (Оба/Статический/Динамический).
Функция: отображение состояния порта маршрутизатора. «Static» означает, что порт маршрутизатора настроен в статическом формате. «Dynamic» означает, что порт маршрутизатора настроен в динамическом формате. «Both» означает, что порт маршрутизатора может работать в обоих форматах.

5. Просмотр списка участников многоадресной рассылки.

		Port Members											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12
1	224.0.1.1	✓		✓									
1	225.10.24.3	✓		✓									
1	226.81.9.8	✓		✓									
1	239.2.11.71	✓		✓									
1	239.5.5.5	✓		✓									
1	239.77.124.213	✓		✓									
1	239.255.255.250	✓		✓									
1	239.255.255.254	✓		✓									

Рис. 178. Отображение списка участников IMGP Snooping

14.1.5. Пример типовой настройки

Как показано на рис. 179, функция IGMP Snooping включена на коммутаторах 1, 2 и 3. На коммутаторах 2 и 3 включена функция автоматического запроса. IP адрес коммутатора 2: 192.168.1.2; IP адрес коммутатора 3: 192.168.0.2, соответственно коммутатор 3 выбран в качестве генератора запросов.

1. Включите функцию IGMP Snooping на коммутаторе 1.
2. Включите функции IGMP Snooping и автоматического запроса на коммутаторе 2.
3. Включите функции IGMP Snooping и автоматического запроса на коммутаторе 3.

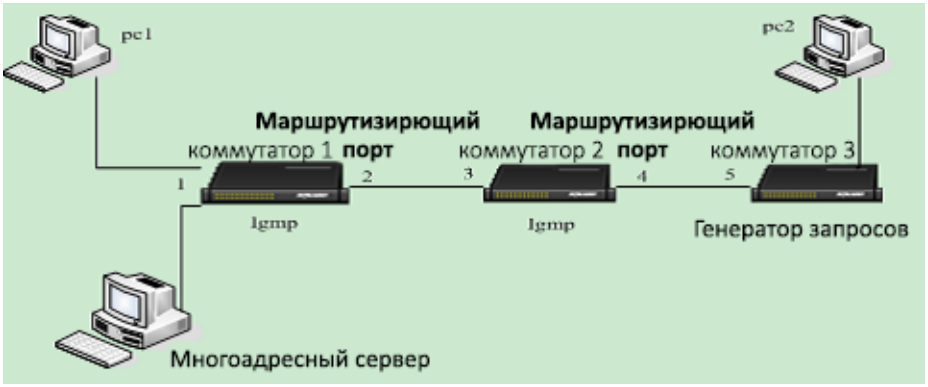


Рис. 179. Пример типовой настройки IGMP Snooping

- Т.к. коммутатор 3 является генератором запросов, он будет периодически отправлять сообщение с общим запросом.
- Порт 4 коммутатора 2 будет принимать это сообщение, соответственно данный порт будет выбран как маршрутизирующий порт. Далее сообщение с запросом будет перенаправлено из порта 3 коммутатора 2 в порт 2 коммутатора 1, который получив это сообщение, будет назначен маршрутизирующим портом.
- Когда PC 1 подключается к многоадресной группе 225.1.1.1, он должен будет отправить сообщение с отчетом участника многоадресной группы коммутатору 1. Соответственно порт 1 и маршрутизирующий порт 2 коммутатора 1 будут подключены к многоадресной группе 225.1.1.1. Затем сообщение с отчетом IMGP будет перенаправлено к коммутатору 2 через маршрутизирующий порт 2. При этом, порты 3 и 4 коммутатора 2 также будут подключены к многоадресной группе 225.1.1.1. Далее сообщение с отчетом IMGP будет перенаправлено к коммутатору 3 через маршрутизирующий порт 4 и порт 5 коммутатора 3 также будет включен в многоадресную группу 225.1.1.1.
- Как только данные от многоадресного сервера достигнут коммутатора 1, они будут перенаправлены к PC 1 через порт 1. Т.к. маршрутизирующий порт 2 также является участником многоадресной группы, данные многоадресной передачи также будут перенаправлены портом 2. Таким образом, когда данные достигнут порта 5 коммутатора 3, пересылка остановится, т.к. отсутствует принимающая сторона. Но,

если PC 2 также является участником 225.1.1.1, к нему также будут перенаправлены данные многоадресной рассылки.

14.2. Протокол GMRP

14.2.1. Введение в GARP

Протокол GARP (Generic Attribute Registration Protocol) используется для распространения, регистрации и удаления определённой информации (VLAN, адреса мультикастовых групп) между коммутаторами в сети.

Благодаря механизму GARP, информация о настройках коммутатора может быть передана по всей локальной сети. Устройства, поддерживающие GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих сообщений «Join» и «Leave». При этом GARP может регистрировать или отменять информацию о настройках других членов в соответствии с их сообщениями «Join/ Leave».

GARP предусматривает три типа сообщений: «Join», «Leave» и «Leave All».

Когда GARP устройство хочет передать свои настройки другим коммутаторам, оно отсылает сообщение «Join». Сообщения «Join» бывают двух типов: «Join Empty» и «Join In». Сообщение «Join In» отправляется для зарегистрированных настроек, в то время как «Join Empty» - для настроек, которые ещё не были зарегистрированы.

Когда GARP устройство хочет удалить свои настройки с других коммутаторов, оно отправляет сообщение «Leave».

После запуска GARP, он начинает отсчитывать период «Leave All». Когда период заканчивается, устройство отсылает сообщение «Leave All».

В качестве приложения указывается порт с поддержкой GARP.

Таймеры GARP включают таймеры «Hold», «Join», «Leave» и «Leave All».

Таймер Hold (Hold Timer): При получении сообщения о регистрации настроек, приложение GARP не отправляет сообщение «Join» сразу, а запускает таймер «Hold». Когда таймер заканчивает отсчёт, приложение отправляет все полученные сообщения о настройках, полученные за этот период в одном «Join» сообщении, что уменьшает количество передаваемых данных по сети.

Таймер Join (Join Timer): чтобы гарантировать, что сообщения «Join» может быть надежно передано другим коммутаторам, коммутатор с включенным GARP будет ожидать временной интервал таймера «Join» после передачи первого сообщения «Join». Если в течение в ответ не получено сообщение «JoinIn», приложение снова отправляет сообщение «Join». В противном случае, сообщение «Join» не отправляется.

Таймер Leave (Leave Timer): Когда коммутатор с включенным GARP хочет, чтобы другие коммутаторы удалили информацию о настройках, он отсылает «Leave» сообщение. Коммутаторы, получившее это сообщение, запускают таймер «Leave». Если они не

получат ни одного сообщения «Join» до истечения времени таймера, коммутаторы удаляют эту информацию о настройках.
Таймер Leave All (LeaveAll Timer): При запуске GARP приложения, запускается таймер «Leave All». По его истечении, приложение отправляет сообщение «Leave All» другим коммутаторам с включенным GARP для того, чтобы они могли перерегистрировать всю свою информацию о настройках. После этого, приложение запускает таймер «LeaveAll» заново, чтобы начать новый цикл.

14.2.2. Протокол GMRP

GARP Multicast Registration Protocol (GMRP) - протокол регистрации многоадресной передачи, основанный на принципах GARP. Он используется для управления информацией о многоадресных группах коммутаторов. Все коммутаторы, поддерживающие GMRP, могут получать регистрационную информацию от других коммутаторов, динамически обновлять информацию о зарегистрированных многоадресных группах, а также передавать собственную регистрационную информацию другим коммутаторам. Механизм обмена информацией гарантирует единообразие информации о многоадресных группах для всех коммутаторов сети.
Если коммутатор регистрирует или отменяет регистрацию в многоадресной группе, порт с поддержкой GMRP передаёт информацию на другие порты в том же VLAN.
Порт-агент (Agent port): обозначает порт, на котором включены функции GMRP и агента.
Порт распространения (Propagation port): обозначает порт, на котором включена только функция GMRP, без функции агента.
Для GMRP необходимо наличие одного и нескольких портов-агентов. Динамически полученные многоадресные записи GMRP и информация об агенте передаётся портом распространения на порты распространения следующих устройств.
Все таймеры GMRP одной сети должны подчиняться одним и тем же правилам во избежание взаимоисключений. Таймеры должны следовать следующим правилам: таймер «Hold»<таймер «Join», 2*таймер «Join»<таймер «Leave», а таймер «Leave»<таймер «Leave All».

14.2.3. Настройка через WEB-интерфейс

1. Глобальная настройка GMRP

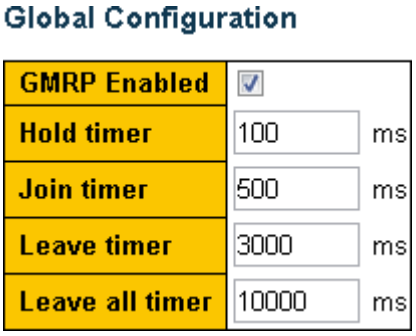


Рис. 180. Глобальная настройка GMRP

Включение GMRP (GMRP Enabled)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: Включение/выключение глобальной функции GMRP.
Таймер (Timer)
Настраиваемые опции: Hold timer/join timer/Leave timer/Leave all timer
Значение по умолчанию: 100/500/3000/10000 мсек.
Функция: настройка значения глобального таймера GMRP.

2. Настройка портов GMRP

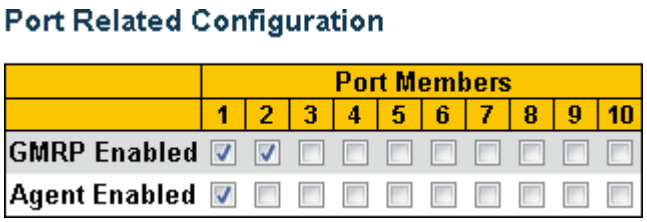


Рис. 181. Настройка портов GMRP

Включение GMRP на порту (GMRP Enabled)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: Включение/выключение функции GMRP на порту.
Включение Агента (Agent Enabled)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Функция: Включение/выключение агента GMRP на порту.

3. Настройка таблицы MAC-адресов агентов

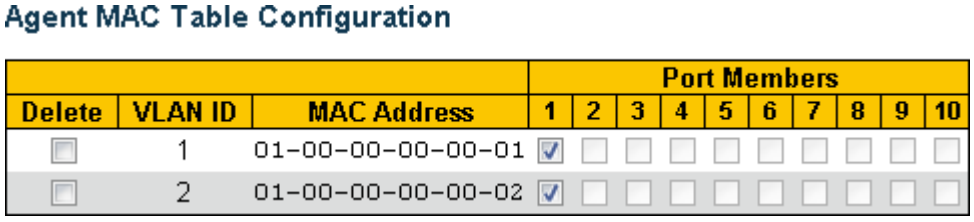


Рис. 182. Настройка таблицы MAC-адресов агента

Функция: настройка MAC-адреса агента, привязанного к порту и VLAN.

4. Таблица статуса MAC-адресов GMRP

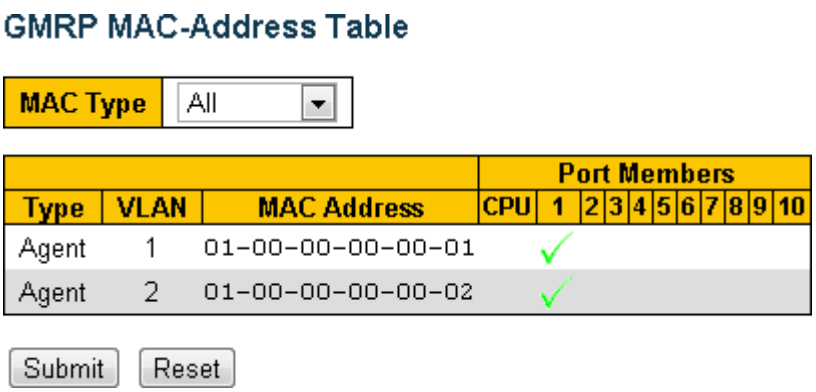


Рис. 183. Таблица статуса MAC-адресов GMRP

Тип MAC_адреса (MAC Type)
Настраиваемые опции: All/Agent/Dynamic
Значение по умолчанию: ALL

14.2.4. Пример типовой настройки

Как показано на рисунке 184, коммутаторы A и B соединены между собой портом 2 каждый. Порт 1 коммутатора A настроен как порт-агент и содержит две многоадресных записи:

- MAC адрес: 01-00-00-00-00-01, VLAN: 1
- MAC адрес: 01-00-00-00-00-02, VLAN: 2

Для того чтобы увидеть динамическую регистрацию между коммутаторами и обновление информации о многоадресной рассылке, необходимо установить различные значение VLAN для портов.

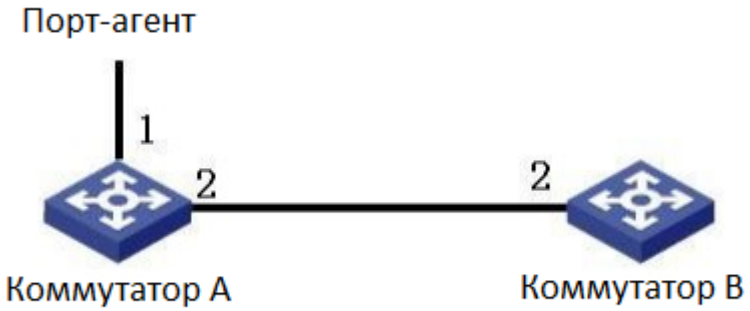


Рис. 184. Сеть GMRP

Настройка коммутатора A:

1. Включите глобальную функцию GMRP на коммутаторе A; используйте значение «Default» для таймера «Leave All» (см. рис. 180);

2. Включите функцию GMRP и функцию агента на порту 1; на порту 2 включите только функцию GMRP; все таймеры должны быть установлены в режим «Default» (см. рис. 181);
3. Настройте запись многоадресного агента. <MAC address, VLAN ID, Member port> настройте как <01 -00-00-00-00-01, 1, 1> и <01 -00-00-00-00-02, 2, 1> (см. рис. 182).

Настройка коммутатора B:

1. Включите глобальную функцию GMRP на коммутаторе B; используйте значение «Default» для таймера «Leave All» (см. рис. 180);
2. Включите функцию GMRP на порту 2; все таймеры должны быть установлены в режим «По умолчанию» (см. рис. 181);

Динамические записи многоадресной передачи GMRP в коммутаторе B показаны в таблице:

Табл. 6.

Подсказка	Тип отображения	Функция	Команда
SWITCH #	Привилегированный режим	Просмотр недавно использованных команд; Просмотр версии программного обеспечения; Просмотр информации для операции ping; Загрузка/Выгрузка файла конфигурации; Восстановление конфигурации по умолчанию; Перезагрузка коммутатора; Сохранение текущей конфигурации; Отобрадение текущей конфигурации; Обновление программного обеспечения.	Введите «**Configure terminal**» для переключения из привилегированного режима в режим настройки Введите «**exit**» для возврата в основной режим
SWITCH (config) #	Режим Настройки	Настроить все функциональные возможности коммутатора	Введите «**exit**» или «**end**» для возврата в привилегированный режим

14.3. Незарегистрированное действие многоадресной рассылки

1. Настройка через WEB-интерфейс

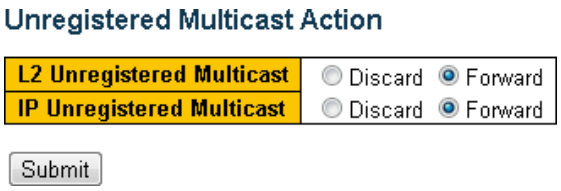


Рис. 185. Незарегистрированное действие многоадресной рассылки

Незарегистрированная многоадресная рассылка L2 (L2 Unregistered Multicast)
Настраиваемые опции: Discard/Forward (Отбросить/Переслать)
Значение по умолчанию: Forward (Переслать)
Незарегистрированная многоадресная рассылка IP (IP Unregistered Multicast)
Настраиваемые опции: Discard/Forward (Отбросить/Переслать)
Значение по умолчанию: Forward (Переслать)

15. Протокол LLDP

15.1. Введение

Протокол Link Layer Discovery Protocol (LLDP) предоставляет собой стандартный механизм обнаружения канального уровня (2-го уровня). Он инкапсулирует различную информацию, например, возможности устройства, адрес, идентификатор устройства и идентификатор интерфейса, в пакет Link Layer Discovery Protocol Data Unit (LLDPDU, блок данных протокола обнаружения уровня канала), и передаёт LLDPDU своим непосредственно подключённым соседям. При получении LLDPDU, соседи сохраняют эту информацию в MIB для запроса и проверки статуса соединения с помощью NMS.

15.2. Настройка с помощью WEB-интерфейса

1. Настройка LLDP.

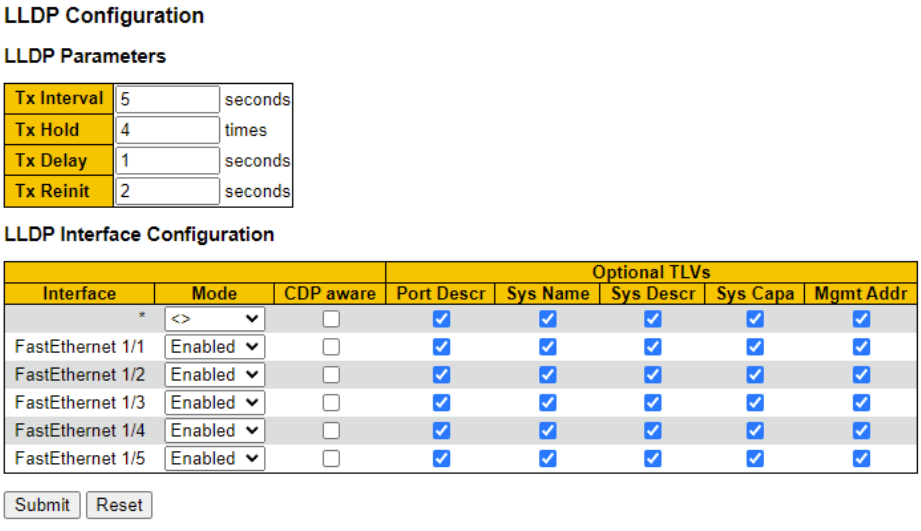


Рис. 186. Настройка LLDP

Интервал передачи (Tx Interval)
Настраиваемый диапазон: 5 ~ 32768 сек.
Значение по умолчанию: 30 сек.
Функция: настройка временного интервала для отправки пакетов LLDP.

Количество удержаний передачи (Tx Hold)
Настраиваемый диапазон: 2 ~ 10 раз.
Значение по умолчанию: 4 раза.
Функция: настройка количества удержаний Tx. Эффективность пакета LLDP = Tx Interval x Tx Hold.

Интервал задержки передачи (Tx Delay)
Настраиваемый диапазон: 1 ~ 8192 сек.
Значение по умолчанию: 2 сек.
Функция: настройка интервала времени передачи между новым пакетом LLDP и предыдущим пакетом LLDP после изменения информации о конфигурации. Значение «Tx Delay» не может быть больше 1/4 значения «Tx Interval».

Интервал реинициализации (Tx Reinit)
Настраиваемый диапазон: 1 ~ 10 сек.
Значение по умолчанию: 2 сек.
Функция: настройка интервала времени передачи между новым пакетом LLDP и предыдущим пакетом LLDP после изменения информации о конфигурации. Значение «Tx Delay» не может быть больше 1/4 значения «Tx Interval».

Режим (Mode)
Опции: Enabled/Disabled/Rx only/Tx only (Включено/Выключено/Только прием/Только передача).
Значение по умолчанию: Enabled (Включено).
Функция: настройка режима пакетов LLDP. «Enabled» означает, что коммутатор может отправлять пакеты LLDP, а также принимать и идентифицировать пакеты LLDP; «Disabled» означает, что коммутатор не отправляет пакеты LLDP и не принимает пакеты LLDP; «Rx only» означает, что коммутатор только принимает и идентифицирует пакеты LLDP; «Tx only» означает, что коммутатор только отправляет пакеты LLDP.

Описание порта (Port Descr)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Enabled (Включено).
Функция: «Enabled» означает, что пакеты LLDP передают описание порта.

Имя системы (Sys Name)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Enabled (Включено).
Функция: «Enabled» означает, что пакеты LLDP передают имя системы.

Описание системы (Sys Descr)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Enabled (Включено).
Функция: «Enabled» означает, что пакеты LLDP передают описание системы.

Возможности системы (Sys Capa)
Опции: Enabled/Disabled (Включено/Выключено).

Значение по умолчанию: Enabled (Включено).
Функция: «Enabled» означает, что пакеты LLDP передают возможности системы.

Адрес управления (Mgmt Addr)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Enabled (Включено).
Функция: «Enabled» означает, что пакеты LLDP передают управляющий адрес.

2. Просмотр информации о соединениях LLDP.

LLDP Neighbor Information

LLDP Remote Device Summary

Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
FastEthernet 1/1	C0-A8-00-1A	20-03				
FastEthernet 1/2	00-01-C1-00-00-00	Fa 1/3	FastEthernet 1/3		Bridge(+)	192.168.0.223 (IPv4)

Рис. 187. Информация LLDP

Для отображения информации LLDP необходимо включить LLDP на двух подключенных устройствах.

16. Настройка MAC-адресов

16.1. Введение

При пересылке пакета коммутатор ищет порт пересылки в таблице MAC-адресов, основываясь на MAC-адресе назначения пакета.
MAC-адрес может быть статическим или динамическим.
Статический MAC-адрес настраивается пользователем. Он имеет наивысший приоритет (динамическими MAC-адресами не отменяется) и действует постоянно.
Коммутатор узнает динамические MAC-адреса при пересылке данных. Они действительны только в течение определенного периода. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра данных для пересылки коммутатор изучает исходный MAC-адрес кадра, организует сопоставление с принимающим портом и запрашивает порт пересылки в таблице MAC-адресов на основе MAC-адреса назначения кадра. Если совпадение найдено, коммутатор пересылает кадр данных с соответствующего порта. Если совпадений не найдено, коммутатор передает кадр в широковещательном формате.
Время старения (Aging time) MAC-адресов начинается с момента добавления динамического MAC-адреса в таблицу MAC-адресов. Если ни один порт не получает кадр с MAC-адресом в течение времени, в 1-2 раза превышающего время старения, коммутатор удаляет запись MAC-адреса из таблицы динамических адресов пересылки. Статические MAC-адреса не подразумевают понятие времени старения.

16.2. Настройка с помощью WEB-интерфейса

1. Настройка времени старения MAC-адресов.

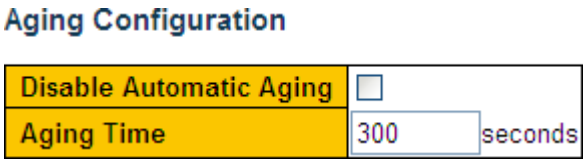


Рис. 188. Настройка времени старения MAC-адресов

Запрет автоматического старения (Disable Automatic Aging)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Enabled (Включено).
Функция: включение и выключение функции старения MAC-адресов. «Enabled» означает, что необходимо настроить время старения. «Disabled» означает, что динамические адреса не устаревают со временем.
Время старения (Aging Time)
Настраиваемый диапазон: 10 ~ 1000000 сек.
Значение по умолчанию: 300 сек.
Функция: настройка время устаревания для динамического MAC-адреса.

2. Настройка динамических MAC-адресов.

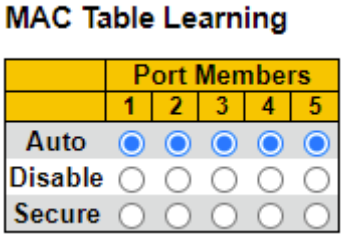


Рис. 189. Настройка динамических MAC-адресов

Порты-участники (Port Members)
Опции: Auto/Disable (Авто/Выключено).
Значение по умолчанию: Auto.
Функция: настройка функции изучения портом динамической таблицы MAC-адресов. «Auto» означает, что порт может изучать динамическую таблицу MAC-адресов. «Disable» означает, что порту запрещено изучать динамическую таблицу MAC-адресов. Изучаются только статические записи MAC-адресов, все остальные кадры отбрасываются.

3. Настройка статических MAC-адресов.

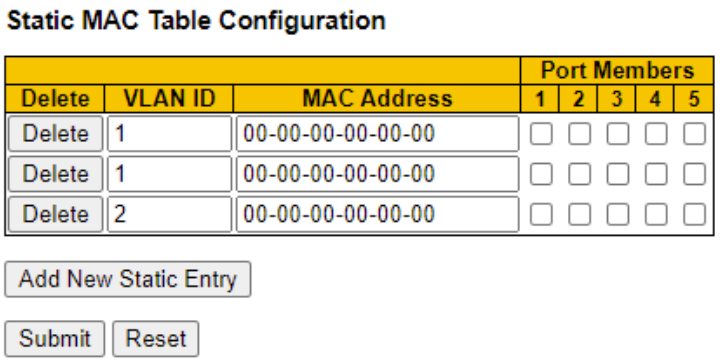


Рис. 190. Настройка статических MAC-адресов

Идентификатор VLAN (VLAN ID)
Опции: все созданные идентификаторы VLAN.
Значение по умолчанию: VLAN 1.
Функция: настройка идентификаторов VLAN статических MAC-адресов.
MAC-адреса (MAC address)
Формат: HH-HH-HH-HH-HH-HH (H - шестнадцатеричное число).
Функция: настройка MAC-адресов. Для MAC-адреса «Unicast» младший бит в первом байте равен 0. Для MAC-адреса «Multicast» младший бит в первом байте равен 1.
Порты-участники (Port Members)
Функция: выбор портов для пересылки пакетов с указанным MAC-адресом назначения.

Нажмите <Add New Static Entry>, чтобы настроить статические MAC-адреса. Поддерживается максимум 64 записи статических MAC-адресов.

4. Просмотр таблицы MAC-адресов.

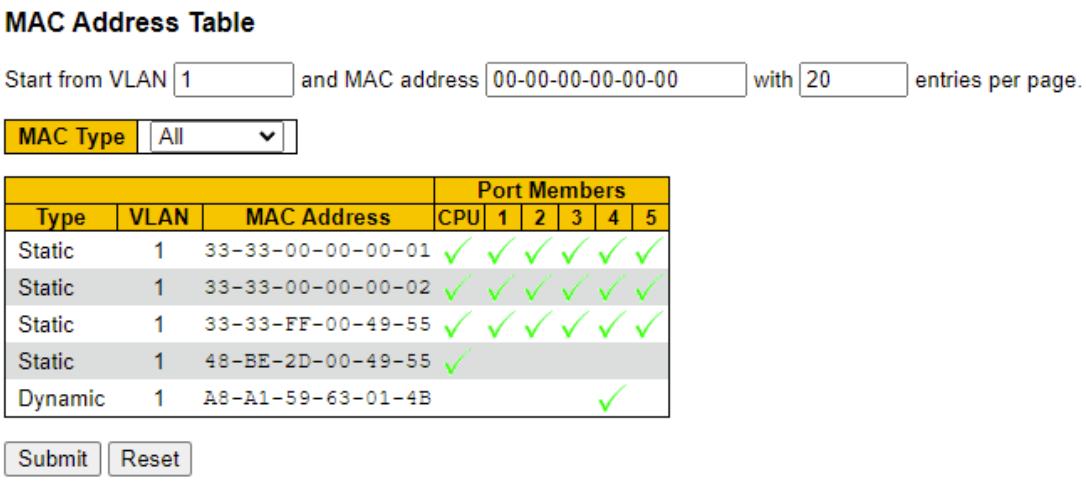


Рис. 191. Отображение таблицы MAC-адресов

17. Виртуальные локальные сети (VLAN)

17.1. Настройка VLAN

17.1.1. Введение

Функция VLAN (Virtual Local Area Networks) делит LAN на несколько логических VLAN. Устройства в одной и той же VLAN могут взаимодействовать друг с другом, а устройства в разных VLAN – нет. Таким образом, широковещательные сообщения ограничены в VLAN, что повышает безопасность локальной сети.
Разделение сети на VLAN не ограничено физическим расположением устройств. Каждая VLAN рассматривается как отдельная логическая сеть. Для передачи данных между двумя разными VLAN необходим маршрутизатор, либо коммутатор 3-го уровня.

17.1.2. Принцип работы

Для того, чтобы сетевые устройства могли различать пакеты из разных VLAN, в кадры добавляются специальные идентификационные поля. На данный момент, самым распространённым протоколом для идентификации VLAN является IEEE802.1Q. Структура кадров 802.1Q показана в таблице:
Табл. 7

DA	SA	802.1Q Header				Length/Type	Data	FCS
		Type	PRI	CFI	VID			

В обычный Ethernet кадр добавляется 4-х байтный заголовок 802.1Q, который служит тегом VLAN.
Тип: 16 бит, используемые для идентификации того, что кадр содержит тег VLAN; значение: 0x8100.
PRI: три бита, определяющие приоритет кадра 802.1p.
CFI: 1 бит, который указывает, инкапсулирован ли MAC-адрес в стандартном формате в различных средах передачи. Значение «0» означает, что MAC-адрес инкапсулирован в стандартном формате, а значение «1» означает, что MAC-адрес инкапсулирован в нестандартном формате.
VID: 12 бит, указывающих номер VLAN в диапазоне значений от 1 до 4093. При этом значения «0», «4094» и «4095» - зарезервированные значения.

- VLAN 1 - это VLAN по умолчанию, Пользователь не может его создать или удалить вручную.
- Зарезервированные номера VLAN нужны для реализации специальных системных функций и также не могут быть созданы или удалены вручную.

Пакет, содержащий заголовок 802.1Q, представляет собой тегированный пакет (Tagged packet); если заголовка нет, то этот пакет нетегированный (Untagged packet). Все пакеты, передаваемые коммутатором, содержат тег 802.1Q.

17.1.3. VLAN на основе портов (Port-based VLAN)

Разделение на VLAN может быть либо по портам, либо по MAC-адресам. Данная серия коммутаторов поддерживает разделение VLAN на основе портов. Данная функция определяет членов VLAN на основе портов коммутатора. После добавления порта в указанную VLAN, порт может пересылать пакеты с тегом для VLAN.

1. Режим порта

Порты делятся на два типа в зависимости от того, как они обрабатывают теги VLAN при пересылке пакетов.

Режим доступа (Access): в режиме доступа порт можно добавить только в одну VLAN. По умолчанию все порты коммутатора являются портами доступа и принадлежат VLAN1. Пакеты, пересылаемые портом доступа, не имеют тегов VLAN. Порты доступа обычно используются для подключения к терминалам, не поддерживающим 802.1Q.

Транковый порт (Trunk): В данном режиме порт можно добавить ко многим VLAN. Транковый порт принимает только тегированные пакеты. При отправке пакетов PVID транковый порт может быть настроен для передачи тега. Он передает тег при отправке других пакетов. Транковые порты обычно используются для подключения сетевых устройств.

Гибридный порт (Hybrid): В гибридном режиме порт может быть добавлен ко многим VLAN. Вы можете настроить тип пакетов, которые будут приниматься гибридным портом, и определить, будет ли передаваться тег, когда гибридный порт отправляет пакеты. Гибридный порт можно использовать ка для подключения сетевых так и пользовательских устройств. Разница между гибридным портом и транковым портом заключается в следующем: гибридный порт не передает тег при отправке пакетов из нескольких VLAN, а транковый порт не передает тег только при отправке пакетов PVID.

2. PVID

Каждый порт имеет атрибут PVID. Когда порт получает нетегированный пакет, он добавляет тег в пакет в соответствии с PVID.

- При настройке PVID порта выберите один из идентификаторов VLAN, разрешенных для данного порта; в противном случае порт может не пересылать пакеты.
- Когда тег PVID добавляется к нетегированным пакетам, вы можете обратиться к настройкам PCP и DEI (см. рис. 60) для получения значений PRI и CFI по умолчанию.

В таблице 8 показано, как коммутатор обрабатывает полученные и отправленные пакеты в соответствии с режимом порта и PVID.

Табл. 8

Обработка полученных пакетов		Обработка пакетов для пересылки	
Нетегированные пакеты	Тегированные пакеты	Тип порта	Обработка пакетов

Добавить теги PVID в пакеты: • если PVID находится в списке разрешенных VLAN, примите пакет; • если PVID отсутствует в списке разрешенных VLAN, отбросьте пакет.	• Если идентификатор (ID) VLAN в пакете находится в списке разрешенных VLAN, принять пакет. • Если идентификатор (ID) VLAN в пакете отсутствует в списке разрешенных VLAN, отбросить пакет.	Access	Пересылка пакета после удаления тега.
		Trunk	Отправка пакета в соответствии с конфигурацией «Egress Tagging»: • Нетегированный порт VLAN (Untag Port VLAN): если идентификатор VLAN в пакете совпадает с PVID и находится в списке разрешенных VLAN, пакет пересылается после удаления тега. Если идентификатор VLAN в пакете отличается от PVID и находится в списке разрешенных VLAN, тег сохраняется и пакет пересылается. • Tag All (тегированные все): если идентификатор VLAN в пакете находится в списке разрешенных VLAN, тег сохраняется и пакет пересылается.
		Hybrid	Отправка пакета в соответствии с конфигурацией «Egress Tagging»: • Untag Port VLAN: действия соответствуют варианту «Trunk». • Tag All: действия соответствуют варианту «Trunk». • Untag All: если идентификатор VLAN в пакете находится в списке разрешенных VLAN, пакет пересылается после удаления тега.

17.1.4. Настройка с помощью WEB-интерфейса

1. Настройка разрешенных VLAN для порта доступа.

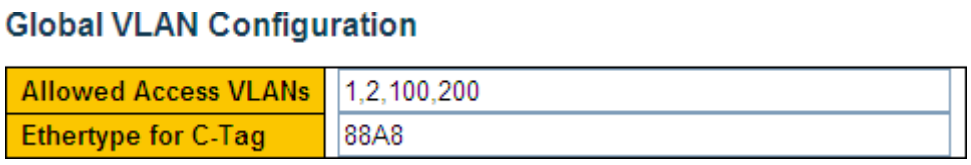
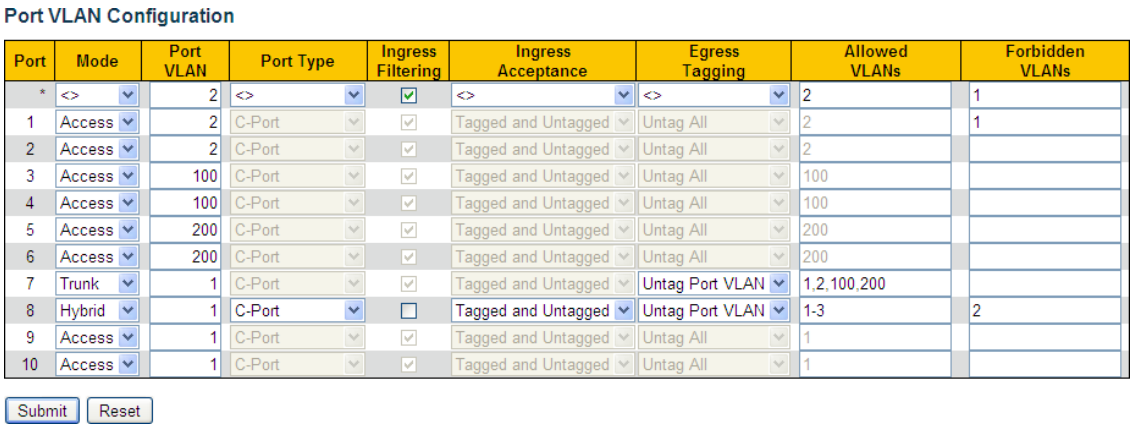


Рис. 192. Отображение таблицы MAC-адресов

Настройка разрешенных VLAN (Allowed Access VLANs)
Настраиваемый диапазон: 1 ~ 4093.

Значение по умолчанию: 1.
Функция: настройка разрешенных VLAN для порта доступа. При наличии нескольких VLAN вы можете разделить VLAN-ы запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая используется для разделения двух непоследовательных идентификаторов VLAN.

2. Настройка порта VLAN.


Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	2	<>	☑	<>	<>	2	1
1	Access	2	C-Port	☑	Tagged and Untagged	Untag All	2	1
2	Access	2	C-Port	☑	Tagged and Untagged	Untag All	2	
3	Access	100	C-Port	☑	Tagged and Untagged	Untag All	100	
4	Access	100	C-Port	☑	Tagged and Untagged	Untag All	100	
5	Access	200	C-Port	☑	Tagged and Untagged	Untag All	200	
6	Access	200	C-Port	☑	Tagged and Untagged	Untag All	200	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,100,200	
8	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-3	2
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Submit Reset

Рис. 193. Настройка порта VLAN

Режим (Mode)
Опции: Access/Trunk/Hybrid.
Значение по умолчанию: Access.
Функция: выбор режима для определенного порта. Каждый порт поддерживает только один режим.
Порт VLAN (Port VLAN PVID)
Настраиваемый диапазон: 1 ~ 4094.
Значение по умолчанию: 1.
Функция: у каждого порта есть PVID. При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID.

- PVID порта доступа должен быть выбран из списка VLAN, разрешенных для этого порта. Настройки VLAN с разрешенным доступом см. на рис. 192.
- PVID транкового или гибридного порта должен быть выбран из списка разрешенных VLAN. См. настройки следующего параметра «Allowed VLANs».

Фильтрация входящих (Ingress Filtering)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение или отключение функции фильтрации входящего трафика гибридного порта. Фильтрация входящих включена принудительно для порта доступа и транкового порта, вы не можете настроить этот параметр. «Enabled»: если идентификатор VLAN в пакете отсутствует в списке разрешенных VLAN, пакет будет отброшен. «Disabled»:

если идентификатор VLAN в пакете отсутствует в списке разрешенных VLAN, пакет будет принят и отправлен на обработку механизму MAC-адресов.

Прием входящего трафика (Ingress Acceptance)

Опции: Tagged and Untagged/ Tagged Only/ Untagged Only.

Значение по умолчанию: Tagged and Untagged.

Функция: настройка типа пакетов, принимаемых гибридным портом. Для порта доступа и транкового порта он принудительно устанавливается в значение «Tagged and Untagged» и не может быть изменен. «Tagged and Untagged» означает, что гибридный порт может принимать пакеты как с тегами, так и пакеты без тегов; «Tagged Only» означает, что гибридный порт принимает только тегированные пакеты и отбрасывает нетегированные пакеты; «Untagged Only» означает, что гибридный порт принимает только нетегированные пакеты и отбрасывает тегированные пакеты.

Тегирование исходящего трафика (Egress Tagging)

Опции: Untag Port VLAN/Unatg All/Tag All.

Значение по умолчанию: Untag Port VLAN.

Функция: настройка обработки передачи пакетов для транкового или гибридного порта. Тегирование исходящего трафика установлено как "Unatg All" принудительно для порта доступа, вы не можете настроить этот параметр. «Untag Port VLAN»: если идентификатор VLAN в пакете совпадает с PVID и находится в списке разрешенных VLAN, пакет пересылается после удаления тега. Если идентификатор VLAN в пакете отличается от PVID и находится в списке разрешенных VLAN, тег сохраняется и пакет пересылается. «Tag All»: если идентификатор VLAN в пакете находится в списке разрешенных VLAN, тег сохраняется и пакет пересылается. «Untag Al»l: если идентификатор VLAN в пакете находится в списке разрешенных VLAN, пакет пересылается после удаления тега.

Разрешенные VLAN-ы (Allowed VLANs)

Настраиваемый диапазон: 1 ~ 4094.

Функция: настройка разрешенных VLAN для транкового/гибридного порта. Когда порт доступа разрешает только одну VLAN, значение этого параметра согласуется со значением «Port VLAN» и не может быть изменено. Если для этого параметра установлено несколько VLAN, вы можете разделить VLAN запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая используется для разделения двух непоследовательных идентификаторов VLAN.

Запрещенные VLAN-ы (Forbidden VLANs)

Настраиваемый диапазон: 1 ~ 4094.

Функция: настройка запрещенных VLAN для порта. После того, как этот параметр установлен для порта, порт никогда не станет портом-участником VLAN, включая динамически зарегистрированную VLAN через GVRP. Если для этого параметра установлено несколько VLAN, вы можете разделить VLAN запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая используется для разделения двух непоследовательных идентификаторов VLAN.

3. Просмотр всех созданных VLAN и портов-участников.

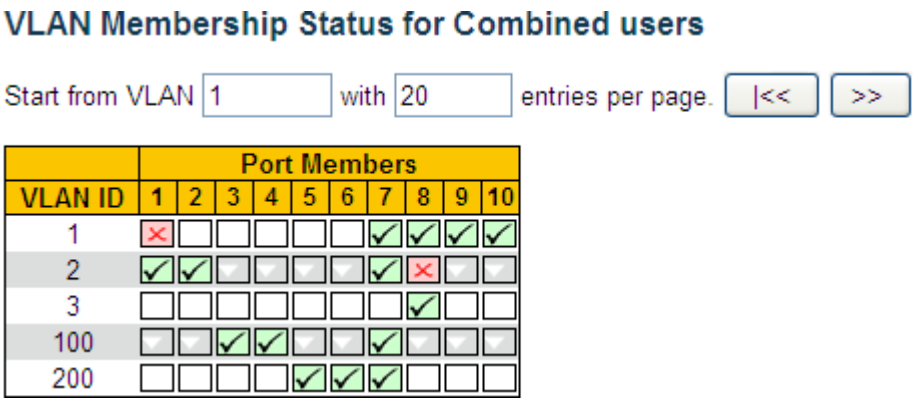
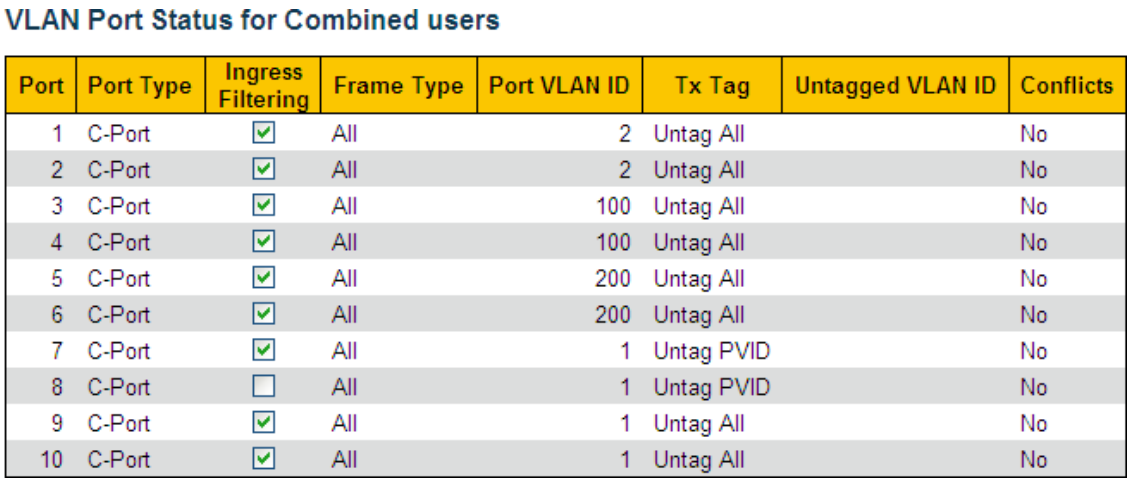


Рис. 194. Отображение всех сознанных VLAN и портов-участников

☑ означает, что порт является портом-участником текущей VLAN; ☒ означает, что текущая VLAN принадлежит к запрещенным VLAN для порта.
На каждой странице может отображаться от 1 до 99 записей VLAN, а по умолчанию отображается 20 записей VLAN. Вы можете указать идентификатор первой записи VLAN на первой странице.

4. Просмотр настроек порта с VLAN



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	2	Untag All		No
2	C-Port	☑	All	2	Untag All		No
3	C-Port	☑	All	100	Untag All		No
4	C-Port	☑	All	100	Untag All		No
5	C-Port	☑	All	200	Untag All		No
6	C-Port	☑	All	200	Untag All		No
7	C-Port	☑	All	1	Untag PVID		No
8	C-Port	☐	All	1	Untag PVID		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No

Рис. 195. Отображение настроек порта с VLAN

17.1.5. Пример типовой настройки

Как показано на рис. 196, сеть разделена на 3 VLAN: VLAN 2, VLAN 100 и VLAN 200. Необходимо, чтобы устройства в одной VLAN могли взаимодействовать друг с другом, при этом другие VLAN были изолированы. ПК не могут различать теги пакетов, поэтому порты коммутаторов A и B, подключенные к ПК, настроены как порты доступа (Access port). Пакеты VLAN 2, VLAN 100 и VLAN 200 должны передаваться между коммутатором A и

коммутатором B, поэтому порты, соединяющие коммутаторы A и B, должны быть настроены как транковые (Trunk port), что позволит транслировать сообщения VLAN 2, VLAN 100 и VLAN 200. В таблице показана конфигурация устройств:

Табл. 9

VLAN	Настройка
VLAN2	Настройте порты 1 и 2 на коммутаторах A и B как порты доступа (Access port), а порт 7 как транковый порт (Trunk port)
VLAN100	Настройте порты 3 и 4 на коммутаторах A и B как порты доступа (Access port), а порт 7 как транковый порт (Trunk port)
VLAN200	Настройте порты 5 и 6 на коммутаторах A и B как порты доступа (Access port), а порт 7 как транковый порт (Trunk port)

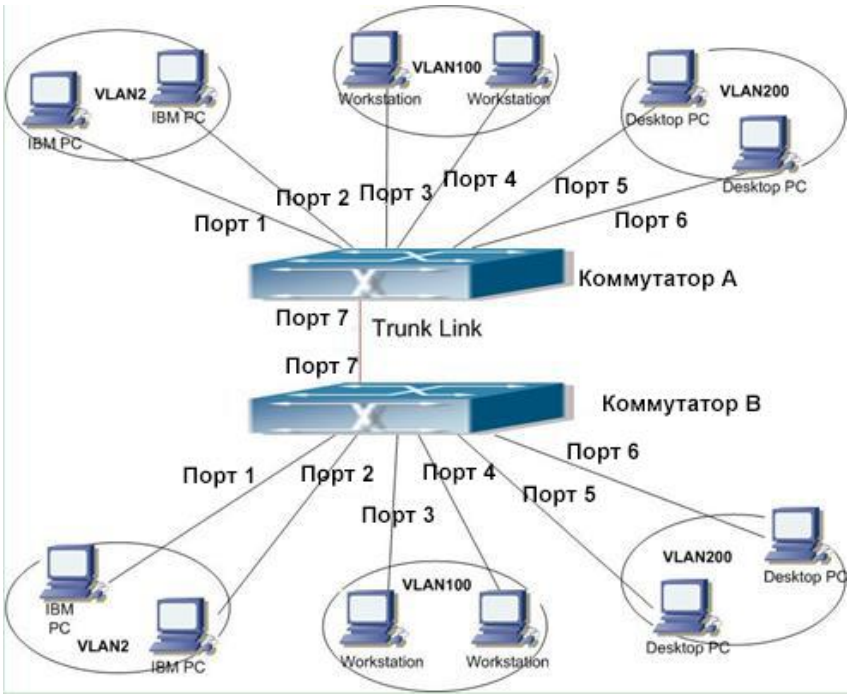


Рис. 196. Настройка VLAN

Настройте коммутаторы A и B, как показано ниже:

1. Настройте VLAN с разрешенным доступом 1,2, 100, 200 (см. рис. 192).
2. Настройте порты 1, 2 как порты доступа, порт VLAN как 2. Настройте порты 3, 4 как порты доступа, порт VLAN как 100. Настройте порты 5, 6 как порты доступа, порт VLAN как 200. Настройте порт 7 как транковый порт, порт VLAN как 1, разрешенные VLAN как 1, 2, 100, 200 (см. рис. 193).
3. Оставьте все остальные параметры по умолчанию.

17.2. Изолированная VLAN (Private VLAN, PVLAN)

17.2.1. Введение

Для реализации комплексной функции изоляции трафика порта, обеспечения безопасности сети и изоляции широковещательного домена PVLAN использует два уровня технологии изоляции.

Верхняя (upper) VLAN - это VLAN с общим доменом, в которой порты являются магистральными (Uplink). Нижняя (lower) VLAN - это VLAN с изолированными доменами, в которых порты являются оконечными (Downlink). Оконечные порты могут быть назначены в различных изолированных доменах, и они могут одновременно устанавливать соединение с магистральным портом. Изолированные домены не могут устанавливать соединение друг с другом.

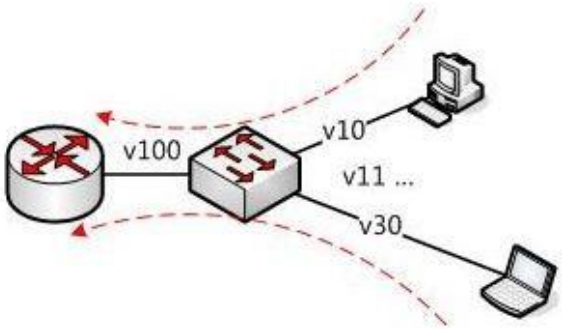


Рис. 197. Схема PVLAN

Как показано на рис. 197, общим доменом является VLAN 100, а изолированными доменами являются VLAN 10 и VLAN 30; устройства в изолированных доменах могут устанавливать соединение с устройством в общем домене, например, VLAN 10 может связываться с VLAN 100; VLAN 30 также может взаимодействовать с VLAN100, но устройства в изолированных доменах не могут устанавливать соединение друг с другом, например, VLAN 10 не может связываться с VLAN 30.

17.2.2. Описание

Функция PVLAN может быть реализована посредством специальной настройки портов.

- PVID магистральных портов совпадает с идентификатором VLAN общего домена; PVID оконечных портов совпадает с их собственным идентификатором VLAN изолированного домена.
- Магистральные порты настроены как гибридные и назначаются в общий домен VLAN и во все изолированные домены; оконечные порты настроены как гибридные и назначаются VLAN в общий домен VLAN и в собственный изолированный домен.
- Пакеты, отправляемые портами-участниками PVLAN, являются нетегированными.

17.2.3. Пример типовой настройки

На рис. 198 показано пример конфигурации PVLAN. VLAN 300 является общим доменом, а порт 1 и порт 2 – магистральными портами; VLAN 100 и VLAN 200 являются изолированными доменами, а порты 3, 4, 5 и 6 являются оконечными портами.

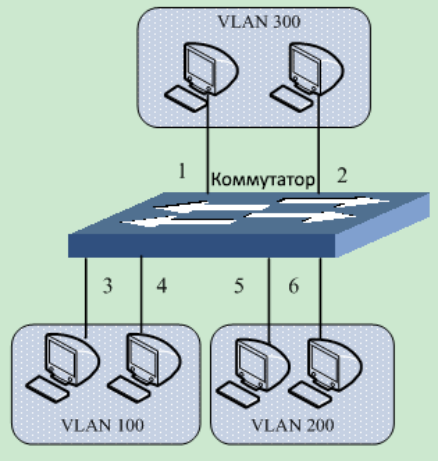


Рис. 198. Пример настройки PVLAN

Настройка коммутатора:

1. Настройте порты 1, 2 как гибридные порты, порт VLAN как 300, тегирование исходящего трафика как «Untag All», разрешенные VLAN как 100,200,300.
2. Настройте порты 3, 4 как гибридные порты, порт VLAN как 100, тегирование исходящего трафика как «Untag All», разрешенные VLAN как 100,300.
3. Настройте порты 5, 6 как гибридные порты, порт VLAN как 200, тегирование исходящего трафика как «Untag All», разрешенные VLAN как 200,300 (см. рис. 199).
4. Оставьте все остальные параметры по умолчанию.

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Hybrid	300	C-Port	☑	Tagged and Untagged	Untag All	100,200,300	
2	Hybrid	300	C-Port	☑	Tagged and Untagged	Untag All	100,200,300	
3	Hybrid	100	C-Port	☑	Tagged and Untagged	Untag All	100,300	
4	Hybrid	100	C-Port	☑	Tagged and Untagged	Untag All	100,300	
5	Hybrid	200	C-Port	☑	Tagged and Untagged	Untag All	200,300	
6	Hybrid	200	C-Port	☑	Tagged and Untagged	Untag All	200,300	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
11	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
12	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Submit Reset

Рис. 199. Настройка портов PVLAN

17.3. Протокол GVRP

17.3.1. Введение в GARP

Протокол GARP (Generic Attribute Registration Protocol) используется для распространения, регистрации и удаления определённой информации (VLAN, адреса мультикастовых групп) между коммутаторами в сети.

Благодаря механизму GARP, информация о настройках коммутатора может быть передана по всей локальной сети. Устройства, поддерживающие GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих сообщений «Join» и «Leave». При этом GARP может регистрировать или отменять информацию о настройках других членов в соответствии с их сообщениями «Join/ Leave».

GARP предусматривает три типа сообщений: «Join», «Leave» и «Leave All».

Когда GARP устройство хочет передать свои настройки другим коммутаторам, оно отсылает сообщение «Join». Сообщения «Join» бывают двух типов: «Join Empty» и «Join In». Сообщение «Join In» отправляется для зарегистрированных настроек, в то время как «Join Empty» - для настроек, которые ещё не были зарегистрированы.

Когда GARP устройство хочет удалить свои настройки с других коммутаторов, оно отправляет сообщение «Leave».

После запуска GARP, он начинает отсчитывать период «Leave All». Когда период заканчивается, устройство отсылает сообщение «Leave All».

В качестве приложения указывается порт с поддержкой GARP.

Таймеры GARP включают таймеры «Hold», «Join», «Leave» и «Leave All».

Таймер Hold (Hold Timer): При получении сообщения о регистрации настроек, приложение GARP не отправляет сообщение «Join» сразу, а запускает таймер «Hold». Когда таймер заканчивает отсчёт, приложение отправляет все полученные сообщения о настройках, полученные за этот период в одном «Join» сообщении, что уменьшает количество передаваемых данных по сети.

Таймер Join (Join Timer): чтобы гарантировать, что сообщения «Join» может быть надежно передано другим коммутаторам, коммутатор с включенным GARP будет ожидать временной интервал таймера «Join» после передачи первого сообщения «Join». Если в течение в ответ не получено сообщение «JoinIn», приложение снова отправляет сообщение «Join». В противном случае, сообщение «Join» не отправляется.

Таймер Leave (Leave Timer): Когда коммутатор с включенным GARP хочет, чтобы другие коммутаторы удалили информацию о настройках, он отсылает «Leave» сообщение. Коммутаторы, получившее это сообщение, запускают таймер «Leave». Если они не получат ни одного сообщения «Join» до истечения времени таймера, коммутаторы удаляют эту информацию о настройках.

Таймер Leave All (LeaveAll Timer): При запуске GARP приложения, запускается таймер «Leave All». По его истечении, приложение отправляет сообщение «Leave All» другим

коммутаторам с включенным GARP для того, чтобы они могли перерегистрировать всю свою информацию о настройках. После этого, приложение запускает таймер «LeaveAll» заново, чтобы начать новый цикл.

17.3.2. Введение в GVRP

Протокол GVRP (GARP VLAN Registration Protocol) является приложением протокола GARP (Generic Attribute Registration Protocol). Он основан на рабочем механизме GARP и управляет динамической регистрацией VLAN на устройстве и обеспечивает распространение информации на другие устройства.
Устройство с включенным протоколом GVRP может получать информацию о регистрации VLAN от других устройств и динамически обновлять локальную информацию о регистрации VLAN, а устройство может распространять локальную информацию о регистрации VLAN к другим устройствам, обеспечивая согласованность информации о VLAN на всех устройствах в одной локальной сети. Информация о регистрации VLAN, распространяемая GVRP, содержит не только локальную статическую регистрационную информацию, заданную вручную, но и динамическую регистрационную информацию от других устройств.

Настройки порта в режиме GVRP и режиме транкового порта являются взаимоисключающими. Порт с поддержкой GVRP не может присоединиться к транковой группе, а на порту, соединяющем транковую группу, нельзя включить GVRP.

17.3.3. Настройка через WEB-интерфейс

1. Включение протокола GVRP и настройка соответствующих таймеров.

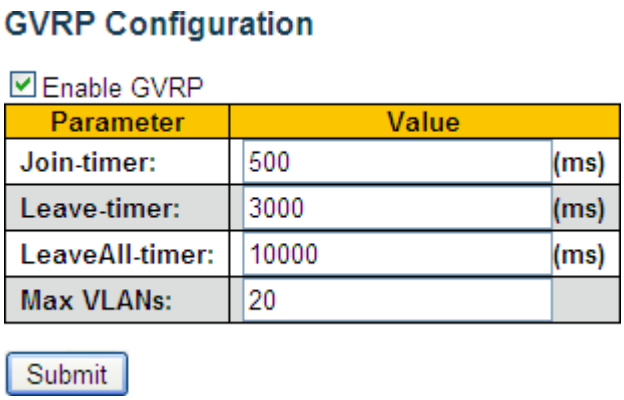


Рис. 200. Настройка протокола GVRP

Включение GVRP (Enable GVRP)
Настраиваемые опции: Enable/Disable (Включено/Выключено).
Значение по умолчанию: Disable (Выключено).
Функция: Включение/Выключение протокола GVRP.

Таймер Join (Join-timer)
Настраиваемый диапазон: 100 ~ 327600 мсек.
Значение по умолчанию: 500 мсек.
Функция: настройка значение таймера «Join». Значение должно быть кратно 100.
Таймер Leave (Leave Timer)
Настраиваемый диапазон: 100 ~ 327600 мсек.
Значение по умолчанию: мсек.
Функция: настройка значение таймера «Leave». Значение должно быть кратно 100.
Таймер LeaveAll (LeaveAll Timer)
Настраиваемый диапазон: 100 ~ 327600 мсек.
Значение по умолчанию: 10000 мсек.
Функция: настройка значение таймера «LeaveAll». Значение должно быть кратно 100.
Описание: если установить тайм-аут таймера «LeaveAll» для разных устройств одинаковым, устройства будут отправлять сообщение «LeaveAll» одновременно, что увеличит количество пакетов. Чтобы этого избежать, фактическое время работы таймера «LeaveAll» должно быть случайным значением и быть длиннее, чем время одного таймера «LeaveAll», но менее чем 1,5 таймера «LeaveAll».
Таймер Hold (Hold Timer)
Настраиваемый диапазон: 1 ~ 4094.
Значение по умолчанию: 20.
Описание: настройка максимального количества VLAN, которые динамически регистрируются с портом GVRP. Для настройки этого параметра необходимо отключить функцию GVRP.

2. Настройка портов GVRP

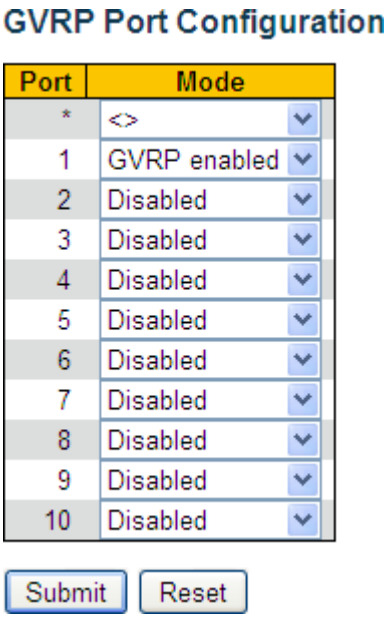


Рис. 201. Настройка портов GVRP

Режим GVRP (Mode)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Описание: включение и выключение режима GVRP на порту.

- Порт GVRP должен быть настроен как транковый порт (Trunk port).
- Порт GVRP используется для передачи атрибутов VLAN других портов GVRP в активном состоянии.

3. Отображение информации о настроенных статически или зарегистрированных динамически VLAN

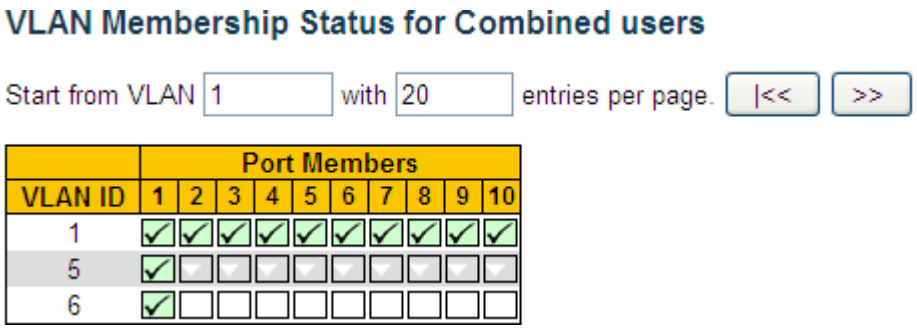


Рис. 202. Информация о VLAN

17.3.4. Пример типовой настройки

Как показано на рис. 203, необходимо включить GVRP на обоих устройствах, чтобы информация о VLAN динамически регистрировалась и обновлялась между устройством A и устройством B.

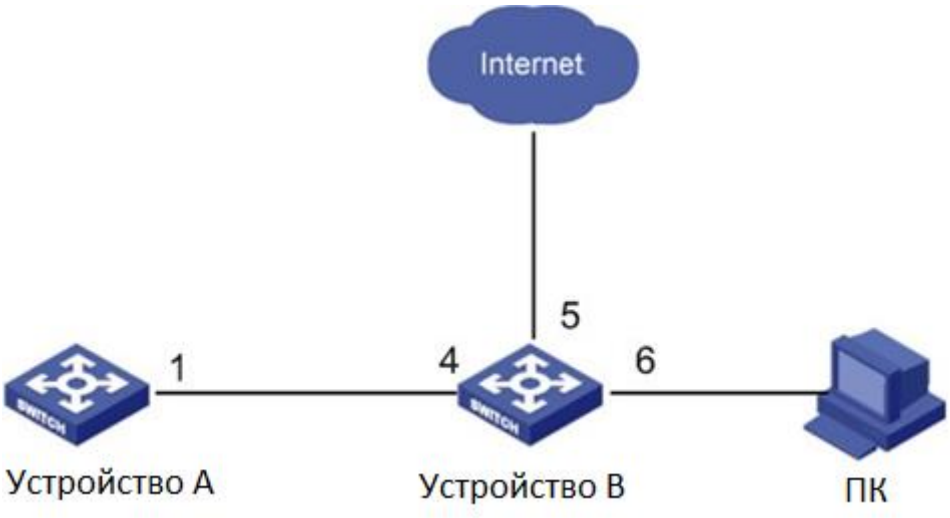


Рис. 203. Пример настройки GVRP

Настройки устройства A:

1. Настройте порт 1 как транковый порт, разрешенный VLAN на 1.
2. Включите глобальный GVRP (см. рис. 200).
3. Включите GVRP на порту 1 (см. рис. 201).

Настройки устройства B:

1. Настройте порт 4 как транковый порт, разрешенный VLAN на 1; настройте порт 5 как порт доступа, разрешенный VLAN на 5; настройте порт 6 как транковый порт, разрешенный VLAN на 1, 6.
2. Включите глобальный GVRP (см. рис. 200).
3. Включите GVRP на портах 4, 5, 6 (см. рис. 201).

Порт 1 коммутатора A может регистрировать ту же информацию о VLAN, что и порт 5 и 6 коммутатора B, как показано на рис. 202.

18. Резервирование

18.1. Протокол Sy2-Ring

18.1.1. Введение

Sy2-Ring и Sy2-Ring+ - проприетарные протоколы резервирования компании Symanitron. Они позволяют сети восстанавливаться менее чем за 50мс при сбое связи, обеспечивая надёжное и стабильное соединение.

Sy2-Ring бывают двух типов: кольцо, определяемое на портах (Sy2-Port-Ring), и кольцо, определяемое по VLAN (Sy2-VLAN-Ring):

- Sy2-Port-Ring: определяет порт, через который необходимо передавать или блокировать пакеты данных.
- Sy2-VLAN-Ring: определяет через который необходимо передавать или блокировать пакеты данных по определённому VLAN. Это позволяет настраивать несколько колец на одном порту, относящихся к разным VLAN.

Sy2-Port-Ring и Sy2-VLAN-Ring нельзя использовать одновременно.

18.1.2. Концепция

Концептуально протоколы работают следующим образом:

Мастер (Master): кольцо может иметь только один узел в статусе «Мастер». Мастер отправляет пакеты протокола Sy2-Ring и следит за текущим статусом кольца. Когда кольцо замкнуто, из двух портов, которые включены в кольцо, один находится в состоянии пересылки, а другой в состоянии блокировки, соответственно.

Ведомый (Slave): кольцо может включать в себя несколько ведомых устройств. Ведомые устройства пересылают пакеты протокола Sy2-Ring и передают «Мастеру» информацию об ошибках.

Резервный порт (Backup port): порт для связи между кольцами называется резервным портом.

Резервный Мастер-порт (Master backup port): когда кольцо имеет несколько резервных портов, резервный порт с большим MAC-адресом является резервным мастер-портом. Он находится в состоянии пересылки.
Ведомый резервный порт (Slave backup port): когда кольцо имеет несколько резервных портов, все резервные порты, кроме резервного мастер-порта, являются ведомыми резервными портами. Они находятся в состоянии блокировки.
Состояние пересылки (Forwarding state): если порт находится в состоянии пересылки, он может получать и отправлять данные.
Состояние блокировки (Blocking state): если порт находится в состоянии блокировки, он может принимать и пересылать только пакеты протокола Sy2-Ring.

18.1.3. Реализация

1. Реализация Sy2-Port-Ring

Порт пересылки на Мастере периодически отправляет пакеты Sy2-Ring для определения состояния кольца. Если резервный порт Мастера получает пакеты, то кольцо замкнуто, если нет, то разомкнуто.
Рабочие процессы коммутаторов A, B, C и D будут следующими:

1. Настройте коммутатор A как Мастер, а другие коммутаторы как Ведомые узлы.
2. Кольцевой порт 1 на Мастере находится в состоянии пересылки, а кольцевой порт 2 находится в состоянии блокировки. Оба порта Ведомого устройства находятся в состоянии пересылки.
3. Если линия связи между коммутаторами C и D неисправна (см. рис. 204):

а) порт 6 и порт 7 на ведомом устройстве находятся в состоянии блокировки. Порт 2 на Мастере переходит в состояние пересылки, обеспечивая работающую линию связи.
б) когда неисправность устранена, порт 6 и порт 7 ведомого устройства находятся в состоянии пересылки. Порт 2 на Мастере переходит в состояние блокировки. Происходит переключение линии связи, и статус сети возвращается к прежней схеме.

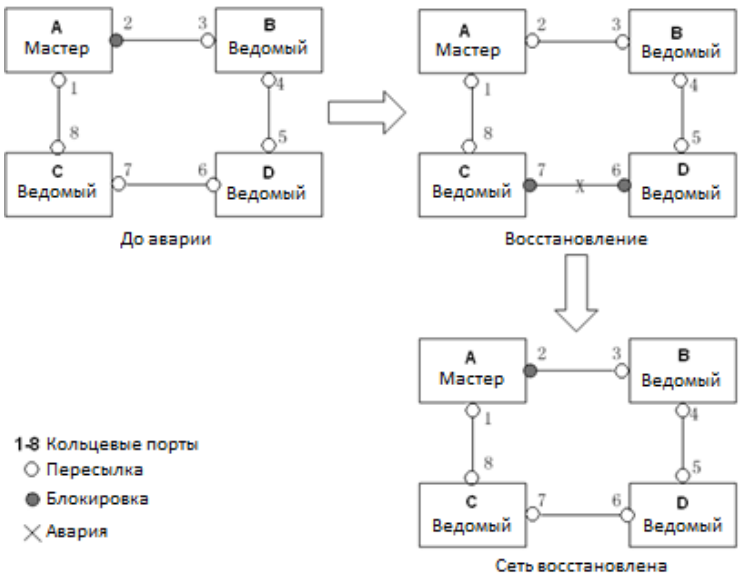


Рис. 204. Диаграмма восстановления сети между коммутаторами C и D

4. Если линия связи между коммутаторами A и C неисправна (см. рис. 205):
а) порт 1 находятся в состоянии блокировки, а порт 2 переходит в состояние пересылки, обеспечивая работающую линию связи.
б) когда неисправность устранена, порт 1 все еще находятся в состоянии блокировки, а порт 8 находится в состоянии пересылки. Переключение в данном случае не происходит.

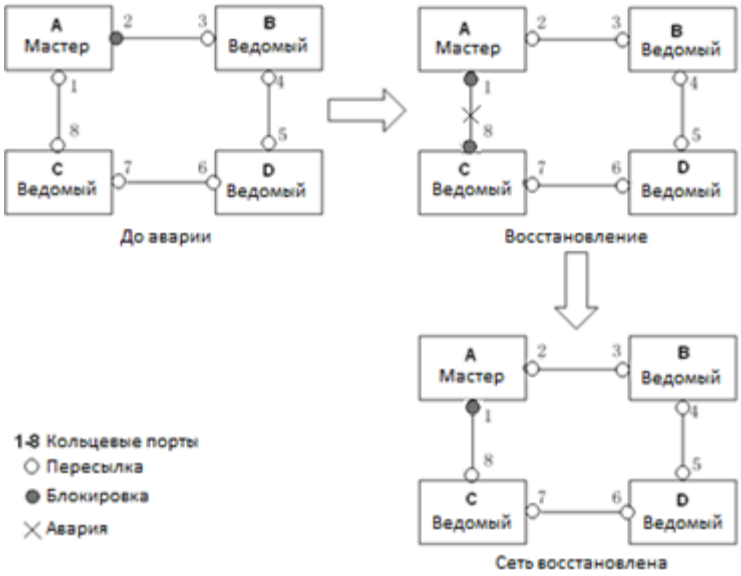


Рис. 205. Диаграмма восстановления сети между коммутаторами A и C

Изменение статуса соединения влияет на статус кольцевых портов.

2. Реализация Sy2-VLAN-Ring
Протокол Sy2-VLAN-Ring дает возможность данным разных VLAN быть переданными различными путями. Каждый путь пересылки для VLAN формируется посредством Sy2-VLAN-Ring. Разные Sy2-VLAN-Ring могут иметь разные мастер-узлы. На рис. 206 показана конфигурация двух Sy2-VLAN-Ring.
Линии связи кольца DT-VLAN 10: AB-BC-CD-DE-EA.
Линии связи кольца DT-VLAN 20: FB-BC-CD-DE-EF.
Два кольца соприкасаются связями BC, CD, DE. Коммутаторы C и D используют одни и те же порты в двух кольцах, но при этом используют разные логические связи, которые основаны на VLAN.

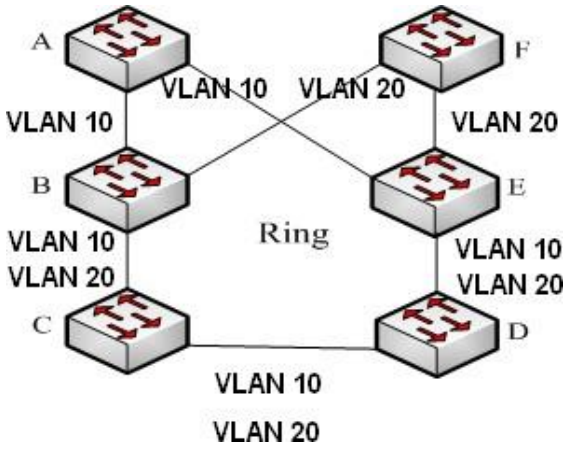


Рис. 206. Sy2-VLAN-Ring

В каждом логическом кольце Sy2-VLAN-Ring реализация идентична реализации Sy2-Port-Ring.

3. Реализация Sy2-Ring+

Протокол Sy2-Ring+ обеспечивает резервирование для двух колец Sy2-Ring. По одному резервному порту настроено на коммутаторе C и коммутаторе D соответственно. Какой порт будет резервным мастер-портом, зависит от MAC-адресов двух портов. Если резервный мастер-порт выходит из строя, его место займёт один из резервных ведомых портов, предотвращая возникновение колец и обеспечивая резервную связь между кольцами.

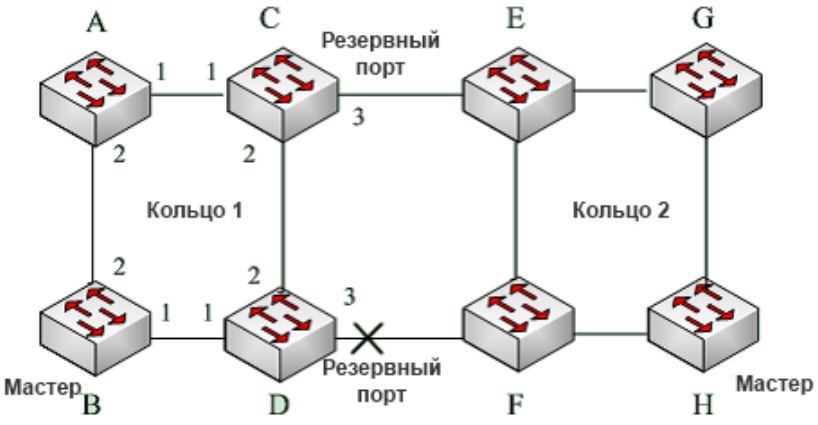


Рис. 207. Топология Sy2-Ring+

18.1.4. Поясняющая информация

Настройки Sy2-Ring должны соответствовать следующим условиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- В каждом кольце может быть только один Мастер и несколько Ведомых.

- На каждом коммутаторе в кольце можно настроить только два порта.
- Если сеть состоит из двух объединенных колец, резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить не более двух резервных портов.
- На коммутаторе в одном кольце может быть настроен только один резервный порт.
- Sy2-Port-Ring и Sy2-VLAN-Ring нельзя настроить на одном коммутаторе одновременно.

18.1.5. Настройка через WEB-интерфейс

1. Настройка режима резервирования Sy2-Ring.

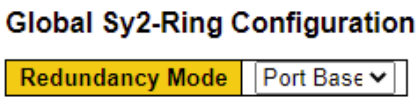


Рис. 208. Настройка режима резервирования

Режим резервирования (Redundancy Mode)
Опции: Port Based/Vlan Based
Значение по умолчанию: Port Based
Функция: выбор режима кольцевого резервирования Sy2-Ring.

- Кольцевые протоколы на основе портов включают RSTP, Sy2-Port-Ring и Sy2-RP-Port, а кольцевые протоколы на основе VLAN включают MSTP, Sy2-VLAN-Ring и Sy2-RP-VLAN.
- Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN.
- Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

2. Настройка Sy2-Port-Ring и Sy2-VLAN-Ring.

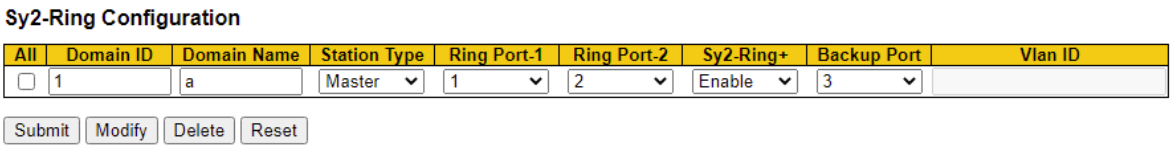


Рис. 209. Настройка Sy2-Port-Ring

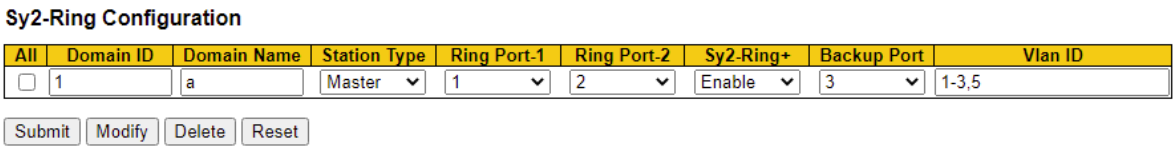


Рис. 210. Настройка Sy2-VLAN-Ring

Идентификатор домена (Domain ID)
Диапазон значений: 1~32
Функция: Идентификатор домена используется для разграничения колец. Один коммутатор поддерживает до 16 колец на основе VLAN. Количество колец на основе портов зависит от количества портов коммутатора.

Имя домена (Domain name)
Диапазон значений: 1 ~ 31
Функция: настройка имени домена.

Тип узла (Station Type)
Опции: Master/Slave (Мастер/Ведомый)
По умолчанию: Master (Мастер)
Функция: выбор роли коммутатора в кольце.

Кольцевой порт 1/Кольцевой порт 2 (Ring Port-1/Ring Port-2)
Варианты: all switch ports (все порты коммутатора)
Функция: Выбор двух кольцевых портов.

- Кольцевой или резервный порт Sy2-Ring и транковый порт являются взаимоисключающими. Кольцевой или резервный порт Sy2-Ring не могут быть назначены на транковый порт, соответственно транковый порт не может быть настроен как кольцевой или резервный порт Sy2-Ring.
- Кольцевые порты между кольцевыми протоколами на основе портов RSTP, Sy2-Ring-Port и Sy2-RP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт Sy2-Ring-Port не могут быть настроены как порт RSTP, кольцевой порт Sy2-RP-Port или порт резервного копирования Sy2-RP-Port. Порт RSTP, кольцевой порт Sy2-RP-Port и резервный порт Sy2-RP-Port не могут быть настроены как кольцевой или резервный порт DT-Ring-Port.
- Не рекомендуется настраивать порты в изолированной группе одновременно как порты Sy2-Ring и резервные порты, а порты Sy2-Ring и резервные порты не могут быть добавлены в изолированную группу.

Sy2-Ring+
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение протокола Sy2-Ring+.

Резервный Порт (Backup Port)
Варианты: all switch ports (все порты коммутатора)
Функция: настройка одного порта в качестве резервного.
Описание: можно настроить резервный порт только после включения функции Sy2-Ring+.

Не настраивайте кольцевой порт в качестве резервного.

Идентификатор VLAN (VLAN ID)
Варианты: all created VLANs (все созданные VLAN)
Функция: настройка одного порта в качестве резервного.

Описание: выбор сети VLAN для кольцевого порта. При наличии нескольких VLAN вы можете разделить VLAN запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая используется для разделения двух непоследовательных идентификаторов VLAN.

3. Просмотр и модификация настроек Sy2-Ring.

Sy2-Ring Configuration

All	Domain ID	Domain Name	Station Type	Ring Port-1	Ring Port-2	Sy2-Ring+	Backup Port	Vlan ID
☐			Master	1	1	Disable	---	
☐	1	a	Master	1	2	Enable	3	---
☐	2	b	Slave	4	5	Disable	---	---

Submit Modify Delete Reset

Рис. 211. Просмотр настроек Sy2-Ring

Выберите запись Sy2-Ring, нажмите <Modify>, чтобы отредактировать конфигурацию Sy2-Ring; нажмите <Delete>, чтобы удалить выбранную запись Sy2-Ring.

4. Отображение статуса портов Sy2-Ring.
Для отображения информации нажмите на любую запись Sy2-Ring.

Sy2-Ring Information

Domain ID	1
Domain Name	a
Station Type	Master
Ring State	Open
Ring Port-1	1 | FORWARD
Ring Port-2	2 | BLOCK
Change Time	0 | Clear
Vlan List	---

Sy2-Ring+ Information

Sy2-Ring+	Enable
Backup Port	3
Device-0	
Backup Port	3 | BLOCK
Equipment IP	192.168.0.2
Equipment MAC	48-be-2d-00-3d-70

Рис. 212. Статус Sy2-Ring

18.1.6. Пример типовой настройки

Как показано на рис. 207, коммутаторы A, B, C, D образуют кольцо 1; коммутаторы E, F, G, H образуют кольцо 2; связи CE и DF являются резервными для колец 1 и 2.

1. Настройка коммутатора A:

Идентификатор домена: 1; Имя домена: A; Тип узла: Slave; Кольцевые порты: 1 и 2; Sy-Ring+: Disable; Резервный порт: не установлен (см. рис.209).

2. Настройка коммутатора B:

Идентификатор домена: 1; Имя домена: A; Тип узла: Master; Кольцевые порты: 1 и 2; Sy-Ring+: Disable; Резервный порт: не установлен (см. рис.209).

3. Настройка коммутаторов C и D:

Идентификатор домена: 1; Имя домена: A; Тип узла: Slave; Кольцевые порты: 1 и 2; Sy-Ring+: Enable; Резервный порт: 3 (см. рис.209).

4. Настройка коммутаторов E, F и G:

Идентификатор домена: 2; Имя домена: B; Тип узла: Slave; Кольцевые порты: 1 и 2; Sy-Ring+: Disable; Резервный порт: не установлен (см. рис.209).

5. Настройка коммутатора H:

Идентификатор домена: 2; Имя домена: B; Тип узла: Master; Кольцевые порты: 1 и 2; Sy-Ring+: Disable; Резервный порт: не установлен (см. рис.209).

18.2. Протокол Sy2-RP

18.2.1. Введение

Компания Symanitron разработала протокол распределенного резервирования (Sy2-RP) для передачи данных в сетях с кольцевой топологией. Реализация данного протокола может помочь предотвратить широковещательные штормы в сетях с кольцевой структурой. Когда канал связи или узел становятся неисправными, резервный канал в режиме реального времени обеспечивает непрерывную передачу данных.

В соответствии со стандартом IEC 62439-6, протокол Sy2-RP использует механизм выбора Мастера без его фиксации. Sy2-RP обеспечивает следующие возможности:

- Время восстановления, не зависящее от масштаба сети.

Sy2-RP обеспечивает время восстановления, не зависящее от масштаба сети за счет оптимизации механизма пересылки пакетов. Sy2-RP обеспечивает восстановление сети в течение 20 мс с предоставлением отчетов о разрывах в реальном времени. Эта функция позволяет коммутаторам обеспечить высокую надежность работы приложений в энергетике, железнодорожном транспорте и многих других отраслях, где требуется управление в режиме реального времени.

- Различные функции проверки линии связи.

Для повышения стабильности сети Sy2-RP предоставляет различные функции проверки линии связи в случае типичных сетевых неисправностей, включая быстрое обнаружение разъединения, проверку качества каналов и проверку состояния оборудования.

- Использование для нескольких сетевых топологий.

Помимо быстрого восстановления простых кольцевых сетей, Sy2-RP также поддерживает сложные кольцевые топологии, такие как пересекающиеся и соприкасающиеся кольца.

Кроме того, Sy2-RP поддерживает решения «multiple instances» на основе VLAN, что позволяет гибко настраивать различные сетевые системы.

- Функции диагностики и управления.

Протокол Sy2-RP включает в себя механизмы запроса состояния и обнаружения аварийных сигналов для диагностики и обслуживания сети, а также механизм предотвращения непреднамеренных операций и неправильных конфигураций, которые могут привести к штормам в кольцевой сети.

18.2.2. Концепция

1. Режимы Sy2-RP.

Sy2-RP включает два режима: Sy2-RP-Port-Based и Sy2-RP-VLAN-Based. Sy2-RP-Port-Based: пересылает или блокирует пакеты на основе определенных портов. Sy2-RP-VLAN-Based: пересылает или блокирует пакеты на основе VLAN. Если порт находится в состоянии блокировки, блокируются только пакеты указанной VLAN. Следовательно, на портах соприкасающегося кольца можно настроить несколько VLAN. Порт может принадлежать разным кольцам Sy2-RP в соответствии с конфигурациями VLAN.

2. Статусы порта Sy2-RP.

Состояние пересылки (Forwarding state): если порт находится в состоянии пересылки, он может принимать и пересылать пакеты данных. Состояние блокировки: если порт находится в состоянии блокировки, он может только принимать и пересылать пакеты Sy2-RP.

Основной порт (Primary port): указывает порт кольца (для корневого коммутатора), статус которого, когда кольцо замкнуто, настроен в формате принудительной пересылки пользователем.

- Если для корневого коммутатора не настроен основной порт, им будет первый порт, состояние связи которого изменилось на «работает» (когда кольцо замкнуто) и он будет состоянии пересылки. Другой порт кольца находится в состоянии блокировки.
- Порт в состоянии блокировки корневого коммутатора может проактивно отправлять пакеты Sy2-RP.

3. Роли Sy2-RP.

Sy2-RP определяет роли коммутаторов путем пересылки пакетов «Announce», предотвращая образование петель на резервных кольцах.

INIT: означает устройство, на котором включен Sy2-RP, а два кольцевых порта находятся в состоянии «Link down».

Root: означает устройство, на котором включен Sy2-RP и, по крайней мере, один порт кольца находится в состоянии «Link up». В кольце корневой коммутатор выбирается в соответствии с содержимым пакетов «Announce». Данная ситуация может измениться в зависимости от топологии сети. Корневой коммутатор периодически отправляет собственные пакеты «Announce» на другие устройства. Статусы кольцевых портов при этом: один кольцевой порт находится в состоянии пересылки, а другой - в состоянии

блокировки. После получения пакета «Announce» от другого устройства корневой коммутатор сравнивает содержимое пакета с содержимым своего собственного пакета «Announce». Если содержимое полученного пакета больше собственного, корневой коммутатор меняет свою роль на обычный или B-Root в соответствии со статусом канала и деградацией CRC на портах.

B-Root: означает устройство, на котором включен Sy2-RP и удовлетворяющее хотя бы одному из следующих условий: один порт кольца находится в состоянии «Link up», а другой в «Link down», деградация CRC, приоритет не менее 200. B-Root сравнивает и пересылает пакеты «Announce». Если содержимое полученного пакета «Announce» меньше, чем содержимое его собственного пакета «Announce», B-Root меняет свою роль на Корневой (Root); в противном случае он пересылает полученный пакет и не меняет своей роли. Статусы кольцевых портов: один кольцевой порт находится в состоянии пересылки.

Обычный (Normal): означает устройство, на котором включен Sy2-RP, а оба кольцевых порта находятся в состоянии «Link up» без деградации CRC и приоритет выше 200. Коммутатор в статусе «Обычный» только пересылает пакеты «Announce», но не проверяет содержимое пакетов. Статусы кольцевых портов: оба кольцевых порта находятся в состоянии пересылки.

Деградация CRC: означает, что количество пакетов CRC превышает пороговое значение в 15 минут.

18.2.3. Реализация

Каждый коммутатор управляет содержимым своего пакета «Announce». Коммутатор с наибольшим количеством значений будет выбран в качестве корневого.

Содержимое пакета «Announce» содержит следующую информацию для назначения ролей.

Табл. 10

Link status	CRC degradation		Role priority	IP address of the device	MAC address of the device
	CRC degradation status	CRC degradation rate			

Статус соединения (Link status): значение установлено на «1», если один порт кольца неактивен и на «0», если оба порта кольца находятся в состоянии соединения.

Статус деградации CRC (CRC degradation status): если деградация CRC происходит на одном порту, значение устанавливается как «1». Если деградация CRC не происходит ни на одном из двух кольцевых портов, значение устанавливается в «0».

Скорость деградации CRC (CRC degradation rate): отношение количества пакетов CRC к пороговому значению в течение 15 минут.

Приоритет роли (Role priority): значение можно установить в веб-интерфейсе.

Параметры в Таблице 10 сравниваются в следующей процедуре:

1. Сначала проверяется значение статуса соединения. Считается, что устройство с большим значением данного статуса связи имеет больший приоритет значения содержимого.
2. Если два сравниваемых устройства имеют одинаковое значение статуса соединения, сравниваются значения статуса деградации CRC. Считается, что устройство с большим значением состояния деградации CRC имеет больший приоритет значения содержимого. Если значение состояния деградации CRC всех сравниваемых устройств равно «1», устройство с большим значением скорости деградации CRC считается имеющим больший приоритет значения содержимого.
3. В случае, если два сравниваемых устройства имеют одинаковое значение статуса соединения и значение деградации CRC, то значения приоритета роли, IP-адресов и MAC-адресов сравниваются последовательно. Считается, что устройство с большим значением имеет больший приоритет значения содержимого.
4. Устройство с большим приоритет значения содержимого выбирается корневым.

Значение скорости деградации CRC участвует в сравнении только когда значение состояния деградации CRC равно «1». В противном случае сравнение происходит независимо от значения скорости деградации CRC.

1. Реализация режима Sy2-RP-Port-Based

Роли коммутаторов будут следующие:

- После запуска все переключатели находятся в состоянии «INIT». Когда состояние одного порта меняется на «Link up», коммутатор становится корневым и отправляет пакеты «Announce» на другие коммутаторы в кольце для подтверждения выбора.
- Коммутатор с наибольшим приоритетом значения содержимого пакета «Announce» выбирается в качестве корневого. Кольцевой порт корневого коммутатора, состояние которого первым становится «Link up», находится в состоянии пересылки, а другой кольцевой порт находится в состоянии блокировки. Среди других коммутаторов в кольце коммутатор с одним кольцевым портом в состоянии «Link down» или деградации CRC является коммутатором B-Root. Коммутатор с обоими кольцевыми портами в состоянии «Link up» и без деградации CRC является «Обычным» (Normal).

Процедура устранения неисправности показана на следующем рисунке

1. В исходной топологии A - это корневой коммутатор; порт 1 находится в состоянии пересылки, а порт 2 - в состоянии блокировки. B, C и D – обычные коммутаторы, а их кольцевые порты находятся в состоянии пересылки.
2. Когда связь между C и D неисправна, Sy2-RP включает для портов 6 и 7 статус блокировки. В результате C и D становятся корневыми коммутаторами. Поскольку коммутаторы A, C и D в настоящий момент являются корневыми, все они отправляют пакеты «Announce». Приоритет значения содержимого коммутаторов C и D больше, чем у A, потому что порт 7 и порт 6 находятся в состоянии «Link down». В данном случае, если приоритет значения содержимого коммутатора D больше, чем приоритет значения содержимого коммутатора C, то коммутатор D выбирается коневым, а коммутатор C становится B-Root. Когда коммутатор D получает пакет «Announce»,

коммутатор A обнаруживает, что приоритет значения содержимого коммутатора D больше, чем его собственный приоритет значения содержимого, а оба его кольцевых порта находятся в состоянии «Link up». Следовательно, коммутатор A становится обычным и назначает статус порта 2 как порт пересылки.

3. Когда связь между коммутаторами C и D восстанавливается, коммутатор D по-прежнему является корневым, потому что его приоритет значения содержимого больше, чем приоритет значения содержимого коммутатора C:

Если на коммутаторе D не настроен основной порт, порт 7 все еще находится в состоянии блокировки, а порт 8 находится в состоянии пересылки.

Если порт 7 на D настроен как основной порт (Primary port), он переходит в состояние пересылки, а порт 8 находится в состоянии блокировки.

Sy2-RP изменяет статус порта 6 на состояние пересылки. В результате коммутатор C становится обычным. Следовательно, при восстановлении канала роли коммутаторов не меняются.

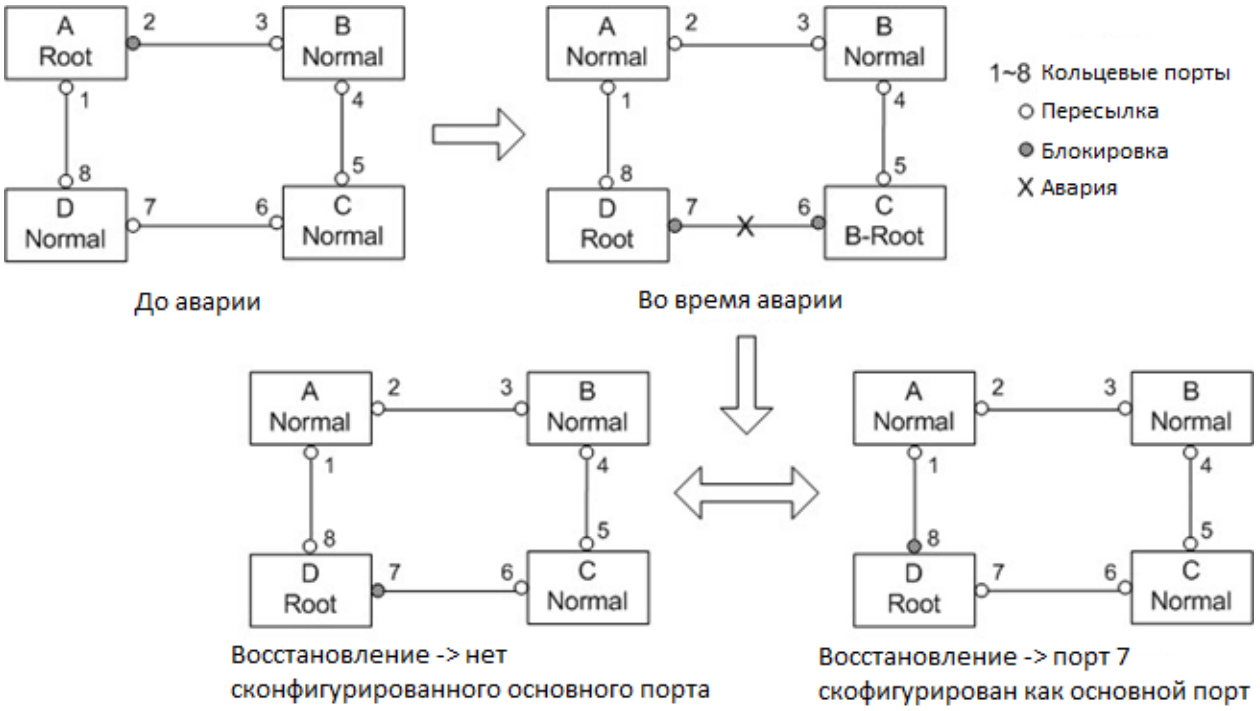


Рис. 213. Восстановление сети с Sy2-RP

В кольцевой сети Sy2-RP роли коммутаторов меняются при сбое линии связи, но не меняются при восстановлении линии связи. Этот механизм повышает безопасность сети и надежность передачи данных.

2. Реализация режима Sy2-RP-VLAN-Based

Кольцо Sy2-RP-VLAN-Based позволяет пересылать пакеты из разных VLAN разными путями. Каждый из путей пересылки для VLAN формирует Sy2-RP-VLAN-Based. Разные кольца на

основе Sy2-RP-VLAN-Based могут иметь разные корневые коммутаторы. Как показано на следующем рисунке, настроены два кольца на основе Sy2-RP-VLAN-Based.
Линии связи кольца Sy2-VLAN10/20-Based: AB-BC-CD-DE-EA.
Линии связи кольца Sy2-VLAN30-Based: FB-BC-CD-DE-EF.
Два кольца соприкасаются связями BC, CD, DE. Коммутаторы C и D используют одни и те же порты в двух кольцах, но при этом используют разные логические связи, которые основаны на VLAN.

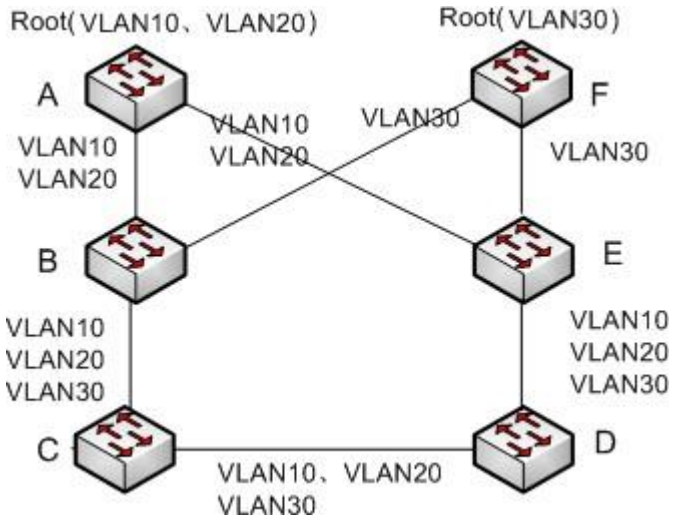


Рис. 214. Sy2-RP-VLAN-Based

В каждом логическом кольце Sy2-RP-VLAN-Based реализация идентична реализации Sy2-RP-Port-Based.

3. Резервирование Sy2-RP

Sy2-RP также может обеспечивать резервное копирование для двух колец Sy2-RP, предотвращая образование петель и обеспечивая нормальную связь между кольцами.
Резервный порт (Backup port): означает порт связи между кольцами Sy2-RP. Можно настроить несколько резервных портов, но они должны находиться в одном кольце. Первый резервный порт в состоянии «Links up» - это главный резервный порт, который находится в состоянии пересылки. Все остальные резервные порты являются ведомыми. Они находятся в состоянии блокировки.
Как показано на рис. 215, на каждом коммутаторе можно настроить один резервный порт. Главный резервный порт находится в состоянии пересылки, а другие резервные порты находятся в состоянии блокировки. Если главный резервный порт или его связь неисправны, для пересылки данных будет выбран ведомый резервный порт.

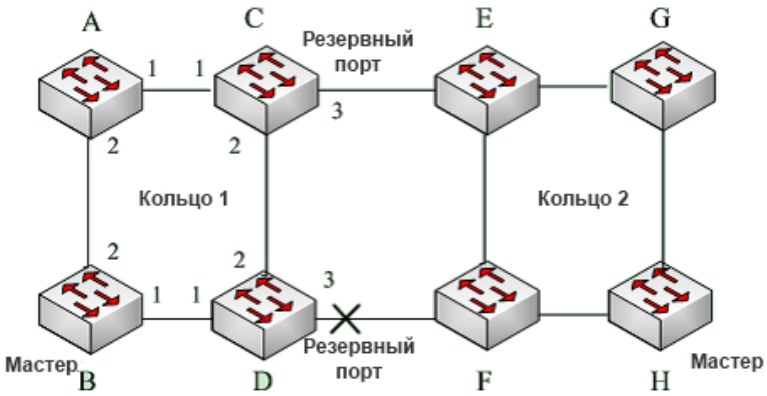


Рис. 215. Резервирование Sy2-RP

*Мастер – корневой коммутатор.

Изменение статуса соединения влияет на статус резервных портов.

18.3. Протокол резервирования Dual Homing

18.3.1. Введение

Как показано на рис. 216, коммутаторы A, B, C и D подключены к кольцу. Протокол Dual Homing выполняет следующие функции, если он включен на коммутаторах A, B, C и D:

- Коммутаторы A, B, C и D могут связываться друг с другом, не влияя на корректную работу устройств в кольце.
- Если связь между коммутаторами A и B неисправна, коммутатор A все еще может связываться с коммутаторами B, C и D через устройства 1 и 2.

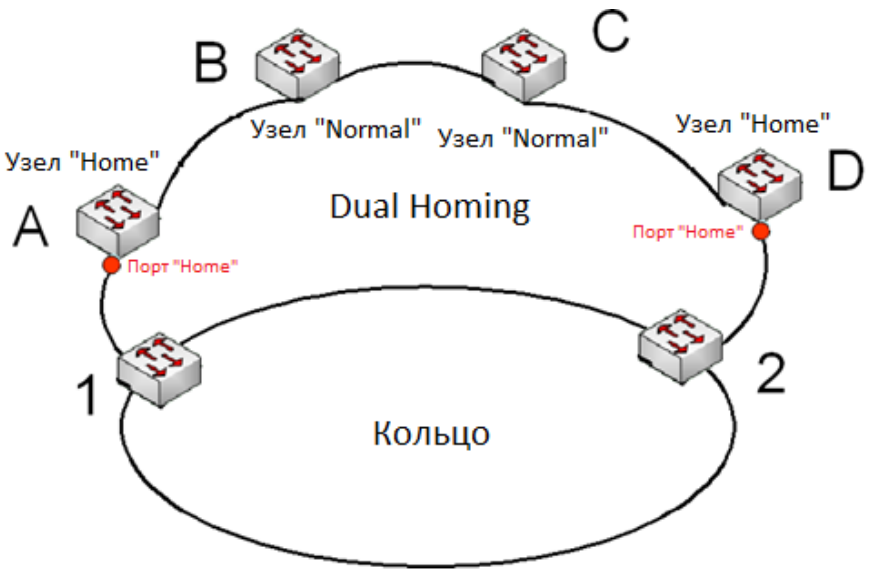


Рис. 216. Реализация протокола Dual Homing

18.3.2. Концепция

Реализация Dual Homing основана на Sy2-RP. Механизм выбора и назначения ролей в Dual Homing такой же, как и в Sy2-RP. Dual Homing обеспечивает резервирование канала связи через настройки узлов «Home», «Normal» и порта «Home».

Узел «Home»: означает устройства, находящиеся на обоих концах канала Dual Homing и принимающих пакеты Sy2-RP.

Порт «Home»: означает порт, соединяющий узел «Home» с внешней сетью. Порт «Home» обеспечивает следующие функции:

- Отправку ответных пакетов корневому коммутатору при получении от него пакетов «Announce». Если корневой коммутатор получает ответные пакеты, он определяет статус кольца как замкнутый. Если корневой коммутатор не получает ответных пакетов, он определяет статус кольца как открытый.
- Блокировку пакетов Sy2-RP внешних сетей и изоляцию канала Dual Homing от внешних сетей.
- Отправку пакетов очистки подключенным устройствам во внешних сетях при изменении топологии канала Dual Homing.

Узел «Normal»: означает все устройства в канале Dual Homing, за исключением крайних устройств, т.е. узлов «Home». Узлы «Normal» передают ответные пакеты узлов «Home».

18.3.3. Реализация

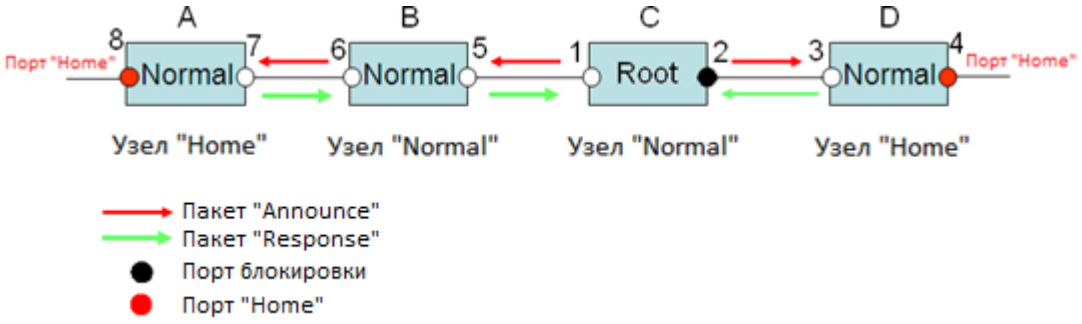


Рис. 217. Конфигурация Dual Homing

Настройки коммутаторов A, B, C и D (см. рис. 216, 217) следующие:

- Конфигурация Sy2-RP: C – корневой коммутатор; порт 2 находится в состоянии блокировки; коммутаторы A, B и D – обычные («Normal»); все остальные порты кольца находятся в состоянии пересылки.
- Конфигурация Dual Homing: коммутаторы A и D – узлы «Home»; порты 8 и 4 являются портами «Home»; коммутаторы B и C - обычные («Normal»).

Реализация:

Корневой коммутатор C отправляет пакеты «Announce» через два своих кольцевых порта. Порты «Home» 8 и 4 получают пакеты «Announce» и отправляют ответные пакеты коммутатору C. Коммутатор C соответственно идентифицирует состояние кольца как закрытое. Порт 2 находится в состоянии блокировки.

Если линия связи между коммутаторами A и B заблокирована, в топологии остаются два канала: A и B-C-D.
Коммутатор A назначается корневым. Порт 7 находится в состоянии блокировки.
В канале B-C-D коммутатор B выбирается в качестве корневого. Порт 6 находится в состоянии блокировки. Коммутатор C становится обычным («Normal»). Порт 2 находится в состоянии пересылки. Коммутатор A может связываться с коммутаторами B, C и D через устройства 1 и 2 (см. рис. 218).

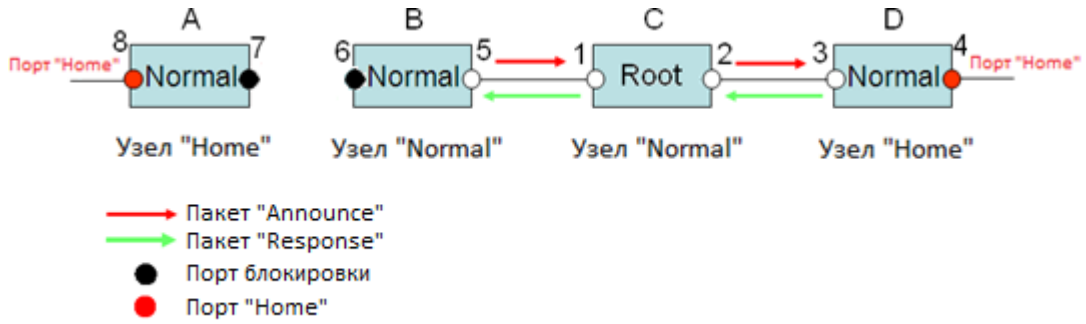


Рис. 218. Восстановление связи с Dual Homing

18.3.4. Описание

Конфигурации Sy2-RP должны соответствовать следующим требованиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- Одно кольцо включает только один корневой коммутатор, но при этом может включать несколько коммутаторов B-Root или «Normal».
- На каждом коммутаторе для кольца можно настроить только два порта.
- Для двух объединенных колец резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить несколько резервных портов.
- На коммутаторе только один резервный порт может быть настроен для одного кольца.

18.3.5. Настройка через WEB-интерфейс

1. Настройка режима резервирования Sy2-RP

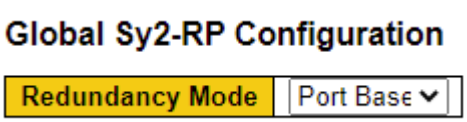


Рис. 219. Настройка режима резервирования Sy2-RP

Режим резервирования (Redundancy Mode)
Опции: Port Based/Vlan Basedë.
Значение по умолчанию: Port Based.
Функция: настройка режима резервирования Sy2-RP.

- Кольцевые протоколы на основе портов включают RSTP, Sy2-Ring-Port и Sy2-RP-Port, а кольцевые протоколы на основе VLAN включают MSTP, Sy2-Ring-VLAN и Sy2-RP-VLAN.
- Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN.
- Кольцевой протокол на основе портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

2. Настройка Sy2-RP-Port и Sy2-RP-VLAN

Рис. 220. Настройка Sy2-RP-Port

Рис. 221. Настройка Sy2-RP-VLAN

Идентификатор домена (Domain ID)
Диапазон значений: 1 ~ 32
Функция: каждое кольцо имеет уникальный идентификатор домена. Один коммутатор поддерживает максимум 8 колец на основе VLAN, количество колец на основе портов зависит от количества портов коммутатора.
Имя домена (Domain name)
Диапазон значений: 1 ~ 31
Функция: настройка имени домена.
Кольцевой порт 1/Кольцевой порт 2 (Ring Port-1/Ring Port-2)
Варианты: all switch ports (все порты коммутатора)
Функция: Выбор двух кольцевых портов.

- Кольцевой порт или резервный порт Sy2-RP и транковый порт являются взаимоисключающими. Кольцевой порт Sy2-RP или резервный порт нельзя добавить к транковому порту; транковый порт не может быть настроен как порт кольца Sy2-RP или резервный порт.
- Кольцевые порты между кольцевыми протоколами на основе портов RSTP, Sy2-Ring-Port и Sy2-RP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт Sy2-RP-Port не могут быть настроены как порт RSTP, кольцевой порт Sy2-Ring-Port или резервный порт Sy2-Ring-Port;

Порт RSTP, порт кольца Sy2-Ring-Port и резервный порт Sy2-Ring-Port нельзя настроить как кольцевой или резервный порт Sy2-RP-Port.

- Не рекомендуется настраивать порты изолированной группе одновременно как порты Sy2-RP и резервные порты, а также порты Sy2-RP и резервные порты не могут быть добавлены в изолированную группу.

Основной порт (Primary Port)
Варианты: --/Ring Port-1/Ring Port-2.
Значение по умолчанию: --
Функция: настройка основного порта. Когда кольцо замкнуто, основной порт корневого коммутатора находится в состоянии пересылки.

Режим Dual Homing (DHP Mode)
Варианты: Disable/Normal-Node/Home-Node.
Значение по умолчанию: Disable (Выключено)
Функция: выключение Dual Homing или настройка режима Dual Homing.

Порт «Home» для Dual Homing (DHP Home Port)
Варианты: Ring-Port-1/Ring-Port-2/Ring-Port-1-2.
Функция: настройка порта «Home» для узла «Home» протокола Dual Homing.
Описание: если в канале Dual Homing есть только одно устройство, оба кольцевых порта узла «Home»должны быть настроены как порт «Home».

Пороговое значение CRC (CRC Threshold)
Диапазон значений: 25 ~ 65535.
Значение по умолчанию: 100.
Функция: настройка порогового значения CRC.
Описание: этот параметр используется при корневого коммутатора. Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет деградацию CRC. В результате значение деградации CRC устанавливается как «1» в содержимом пакета «Announce» порта.

Приоритет роли (Role Priority)
Диапазон значений: 0 ~ 255.
Значение по умолчанию: 128.
Функция: настройка приоритета коммутатора.

Резервный Порт (Backup Port)
Варианты: all switch ports (все порты коммутатора)
Функция: настройка резервного порта.

Не настраивайте кольцевой порт как резервный порт.

Список VLAN (VLAN List)
Варианты: all created VLANs (все созданные VLAN)
Функция: выбор сети VLAN, управляющих текущим кольцом Sy2-RP-VLAN.

Идентификатор VLAN (Protocol Vlan ID)
Диапазон значений: 1 ~ 4093.
Функция: идентификатор VLAN должен быть одним из служебных VLAN.
Описание: пакеты Sy2-RP с идентификатором VLAN служат основой для диагностики и обслуживания кольца Sy2-RP-VLAN.

3. Просмотр и модификация Sy2-RP.

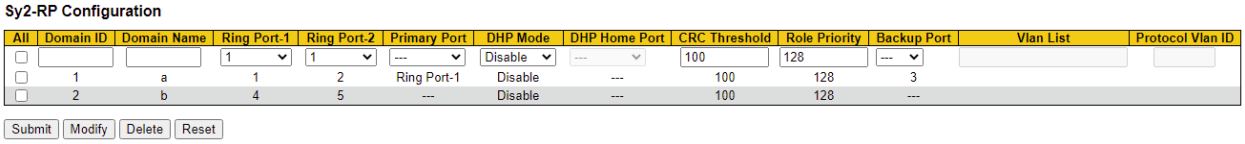


Рис. 222. Отображение и модификация Sy2-RP

Выберите запись Sy2-RP, нажмите <Modify>, чтобы изменить настройки соответствующего Sy2-RP; нажмите <Delete>, чтобы удалить указанную запись Sy2-RP.

4. Отображение Sy2-RP и статуса порта
Нажмите соответствующую запись Sy2-RP для отображения информации.

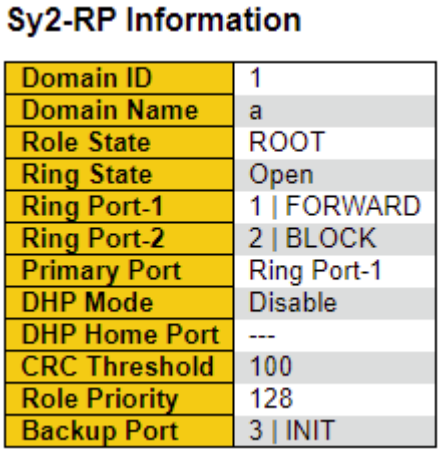


Рис. 223. Статус Sy2-RP

18.3.6. Пример типовой настройки

Как показано на рис. 215, коммутаторы A, B, C, D образуют кольцо 1; коммутаторы E, F, G, H образуют кольцо 2; связи CE и DF являются резервными для колец 1 и 2.
1. Настройка коммутаторов A и B:
Идентификатор домена: 1; Имя домена: A; Кольцевые порты: 1 и 2; Сохраните значения по умолчанию для приоритета роли и резервного порта (см. рис.220).
2. Настройка коммутаторов C и D:

Идентификатор домена: 1; Имя домена: A; Кольцевые порты: 1 и 2; Резервный порт: 3; Оставьте значение по умолчанию для приоритета роли (см. рис.220).

3. Настройка коммутаторов E, F, G и H:

Идентификатор домена: 2; Имя домена: B; Кольцевые порты: 1 и 2; Сохраните значения по умолчанию для приоритета роли и резервного порта (см. рис.220).

18.4. Протоколы STP/RSTP

18.4.1. Введение

Протокол STP (Spanning Tree Protocol) основан на стандарте IEEE802.1D и разработан для предотвращения широковещательных штормов, вызванных циклическими соединениями, а также используется для резервирования связей. Устройства, поддерживающие STP, обмениваются служебными пакетами и блокируют определённые порты для разрыва "петель" и создания "деревьев", предотвращая бесконечную передачу данных по кругу. Недостатком STP является то, что он не поддерживает быстрый переход порта в рабочее состояние и существует необходимость выдерживать техническую паузу перед переходом в режим пересылки.

Для решения проблемы с протоколом STP, IEEE разработал стандарт 802.1w в качестве дополнения стандарта 802.1D. IEEE802.1w даёт определение протоколу Rapid Spanning Tree Protocol (RSTP). По сравнению с STP, RSTP работает быстрее за счёт добавления альтернативных и резервных портов для корневых и назначенных портов соответственно. Когда корневой порт/порт назначения выходит из строя, его альтернативный порт/резервный порт немедленно переходит в состояние пересылки.

18.4.2. Концепция

Корневой мост (Root bridge): является “корнем дерева”. Сеть может иметь только один корневой мост. Какой из коммутаторов будет корневым зависит от сетевой топологии и данная ситуация может измениться при изменении топологии сети. Для определения сетевой целостности, корневой коммутатор периодически отправляет BPDU другим узлам, которые пересылают их дальше, чтобы гарантировать стабильность топологии.

Корневой порт (Root port): порт некорневого коммутатора, расстояние от которого до корневого коммутатора наименьшее. Под наименьшим расстоянием понимается расстояние до корневого коммутатора с наименьшей стоимостью пути. Все коммутаторы сети связываются с корневым коммутатором через корневые порты. При этом у всех некорневых устройств может быть только один корневой порт. На корневом коммутаторе корневых портов нет.

Порт назначения (Designated port): порт на мосту назначения, который отвечает за пересылку конфигурации BPDU другому устройству или локальной сети. Все порты в корневом мосту являются портами назначения.

Альтернативный порт (Alternate port): резервный порт корневого порта. Если корневой порт выходит из строя, альтернативный порт становится новым корневым.

Резервный порт (Backup port): резервный для порта назначения. Когда порт назначения выходит из строя, резервный порт становится новым портом назначения и передаёт данные вместо него.

18.4.3. BPDU

Для предотвращения петель все устройства в сети совместно вычисляют структуру логического дерева (ST). Они подтверждают топологию сети путем доставки сообщений BPDU между собой. В таблице 11 показана структура данных BPDU.

Табл. 11

…	Root bridge ID	Root path cost	Designated bridge ID	Designated port ID	Message age	Max age	Hello time	Forward delay	…
…	8 bytes	4 bytes	8 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	…

Структура данных BPDU включает:

Идентификатор корневого моста (Root bridge ID): приоритет корневого коммутатора (2 байта) + MAC-адрес корневого коммутатора (6 байт).

Стоимость пути (Root path cost): стоимость кратчайшего пути до корневого моста.

Идентификатор моста назначения (Designated bridge ID): приоритет назначенного коммутатора (2 байт) + MAC-адрес моста назначения (6 байт).

Идентификатор порта назначения (Designated port ID): приоритет порта + номер порта.

Возраст сообщения (Message age): как далеко BPDU может быть передан по сети.

Максимальный возраст или время старения (Max age): максимальное время хранения BPDU на устройстве. Когда возраст сообщения больше чем время старения, BPDU отбрасывается.

Интервал Hello (Hello time): интервал времени для отправки BPDU.

Задержка отправки (Forward delay): задержка изменения статуса (отбрасывание--обнаружение--пересылка).

18.4.4. Реализация

Процесс вычисления логического дерева для всех устройств следующий:

1. Начальная стадия: все устройства на всех своих портах генерируют BPDU, считая себя корневым мостом; ID корневого моста – это ID устройства; стоимость пути до корневого коммутатора равна 0; ID моста назначения – это ID устройства, порт назначения – локальный порт.
2. Выбор оптимальной конфигурации BPDU. Все устройства отсылают свои BPDU и получают BPDU от других устройств. При получении BPDU, каждый порт сравнивает полученный BPDU со своим.
   - Если приоритет конфигурации BPDU, сгенерированного локальным портом выше, чем принятые настройки BPDU, устройство не выполняет никакой обработки.
   - Если приоритет конфигурации BPDU, сгенерированный локальным портом, ниже, чем принятая конфигурация BPDU, устройство заменит содержимое BPDU

конфигурации, сгенерированное локальным портом, содержимым принятой конфигурации BPDU.

Устройство выбирает оптимальную конфигурацию BPDU после сравнения конфигурации BPDU всех портов. Принципы сравнения BPDU:

- Конфигурация BPDU с наименьшим идентификатором корневого моста имеет наивысший приоритет
- Если ID корневого коммутатора двух BPDU одинаковы, сравнивается стоимость пути до корневого коммутатора. Если стоимость пути до корневого коммутатора плюс стоимость пути до локального порта меньше, приоритет BPDU выше.
- Если стоимость пути до корневого коммутатора также одинаковы, по порядку сравниваются ID назначенных коммутаторов, ID назначенных портов и ID портов, получивших BPDU. BPDU с наименьшим ID будет иметь наивысший приоритет.

3. Выбор корневого моста. Корневым коммутатором логического дерева (spanning tree) является устройство с наименьшим идентификатором (ID) устройства.
4. Выбор корневых портов. Некорневые коммутаторы сделают свои порты, получающие наилучшую конфигурацию BPDU, корневыми.
5. Вычисление конфигурации BPDU порта назначения. В соответствии с конфигурацией BPDU и стоимостью пути корневого порта, конфигурация BPDU порта назначения рассчитывается для каждого порта:
   - Идентификатор корневого моста заменяется идентификатором конфигурации BPDU корневого порта.
   - Стоимость корневого пути заменяется на стоимость конфигурации BPDU корневого порта плюс соответствующая стоимость пути корневого порта.
   - ID моста назначения заменяется ID устройства.
   - ID порта назначения заменяется на ID данного порта.
6. Выбор порта назначения. Если вычисленное значение BPDU лучше, устройство делает этот порт назначенным, заменяет BPDU порта вычисленным и отправляет новый BPDU. Если текущее значение BPDU лучше, устройство не обновляет его и блокирует порт. Заблокированные пакеты могут принимать и отправлять только техническую информацию RSTP, но не данные.

18.4.5. Настройка через WEB-интерфейс

1. Настройка параметров сетевого моста

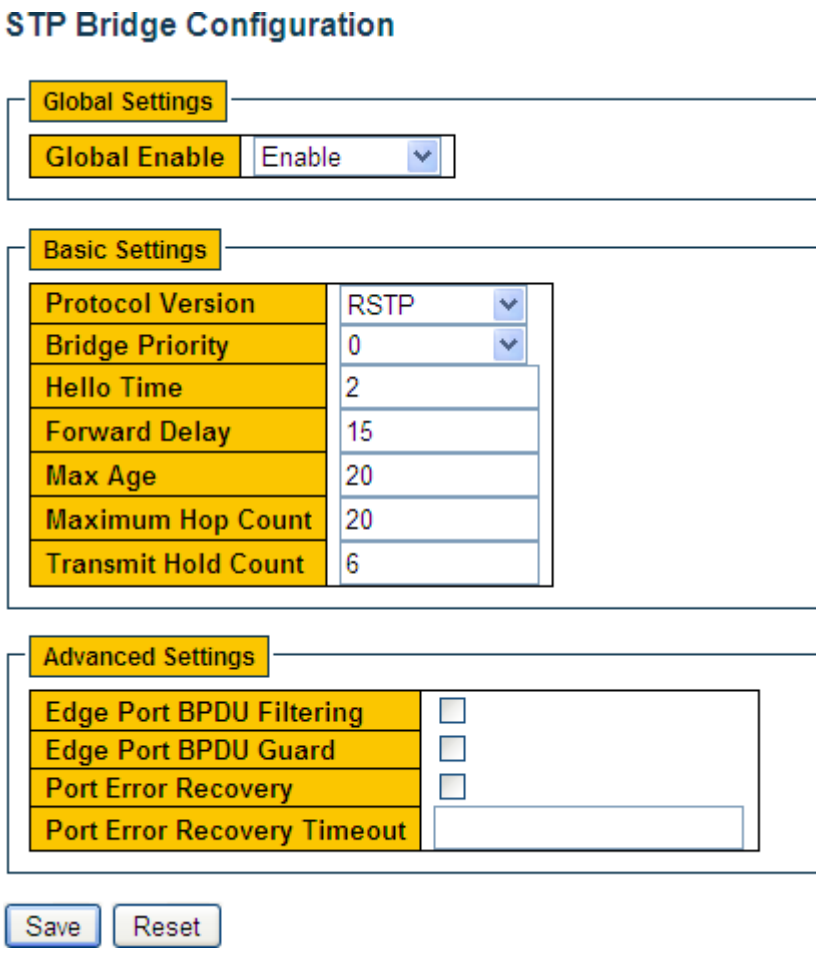


Рис. 224. Настройка параметров сетевого моста

Глобальное включение (Global Enable)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: глобальное включение и выключение STP.

- Кольцевые протоколы на основе портов включают RSTP, Sy2-Ring-Port и Sy2-RP-Port, а кольцевые протоколы на основе VLAN включают MSTP, Sy2-Ring-VLAN и Sy2-RP-VLAN.
- Кольцевые протоколы на основе портов и на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только один режим кольцевого протокола.

Приоритет протокола (MSTP/RSTP/STP)
Опции: MSTP/RSTP/STP.

Значение по умолчанию: MSTP.
Функция: выбор протокола.

Приоритет моста (Brigde Priority)

Настраиваемый диапазон: 0 ~ 61440 с шагом 4096.
Значение по умолчанию: 32768.
Функция: настройка приоритета сетевого моста
Описание: приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.

Интервал времени Hello (Hello Time)

Настраиваемый диапазон: 1 ~ 10 сек.
Значение по умолчанию: 2 сек.
Функция: Настройка временного интервала отправки настроек BPDU.

Время задержки (Forward Delay)

Настраиваемый диапазон: 4 ~ 30 сек.
Значение по умолчанию: 15 сек.
Функция: время изменения статуса от Отбрасывания (Discarding) до Изучения (Learning) и от Изучения (Learning) до Пересылки (Forwarding).

Максимальное возраст или время старения (Max Age)

Настраиваемый диапазон: 6 ~ 40 сек.
Значение по умолчанию: 20 сек.
Функция: максимальная продолжительность, в течение которой BPDU может быть сохранен на устройстве.
Описание: Если значение возраста сообщения в BPDU больше указанного значения, тогда BPDU отбрасывается.

- Значения Forward Delay Time, Hello Time и Max Age Time должны соответствовать следующим требованиям: 2 * (Forward Delay Time – 1 сек.) > = Max Age Time; Максимальное время возраста > = 2 * (время приветствия + 1 сек.).
- Рекомендуется настройка по умолчанию.

Счетчик задержки передачи (Transmit Hold Count)

Настраиваемый диапазон: 1 ~ 10.
Значение по умолчанию: 6.
Функция: настройка максимального количества пакетов BPDU, которые могут быть отправлены портом в течение каждого интервала «Hello».

Фильтрация BPDU на граничном порту (Edge Port BPDU Filtering)

Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключения режима получения и отправки граничным портом пакетов BPDU.

Защита от BPDU на граничном порту (Edge Port BPDU Guard)

Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).

Функция: режим контроля перехода граничного порта в отключенное состояние из-за получения ошибок и перезагрузку при приеме пакетов BPDU.

Восстановление порта (Port Error Recovery)

Опции: Enabled/Disabled (Включено/Выключено).

Значение по умолчанию: Disabled (Выключено).

Функция: включение или выключение режима автоматического восстановления порта из состояния ошибки в нормальное состояние.

Тайм-аут восстановления порта (Port Error Recovery Timeout)

Настраиваемый диапазон: 30 ~ 86400 сек.

Функция: настройка времени восстановления порта из состояния ошибки до нормального состояния.

2. Настройка порта RSTP.

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
*	☐	<>		<>	<>	☑	☐	☐	☐	<>
1	☑	Specific	5	128	Non-Edge	☑	☐	☐	☐	Auto
2	☑	Specific	10	128	Non-Edge	☑	☐	☐	☐	Auto
3	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
4	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
5	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
6	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
7	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
8	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
9	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
10	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
11	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
12	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto

Submit Reset

Рис. 225. Настройка порта RSTP

Включение STP (STP Enabled)

Опции: Enabled/Disabled (Включено/Выключено).

Значение по умолчанию: Disabled (Выключено).

Функция: включение и выключение STP/RSTP на порту.

- Порт RSTP и транковый порт являются взаимоисключающими. Порт RSTP нельзя добавить к транковому порту; транковый порт не может быть настроен как порт RSTP.
- Кольцевые порты между кольцевыми протоколами на основе портов RSTP, Sy2-Ring-Port и Sy2-RP-Port являются взаимоисключающими, то есть порт RSTP не может быть настроен как кольцевой или резервный порт Sy2-RP-Port/Sy2-Ring-Port или Sy2-RP-Port/Sy2-Ring-Port; кольцевой и резервный порт Sy2-RP-Port/Sy2-Ring-Port не могут быть настроены как порт RSTP.

- Не рекомендуется, чтобы порты в изолированной группе были одновременно настроены как порты RSTP, а порты RSTP не могут быть добавлены в изолированную группу.

Стоимость пути (Path Cost)
Настраиваемый диапазон: Auto/Specific 1 ~ 200000000.
Значение по умолчанию: Auto.
Функция: стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от пропускной способности. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение, вручную выберите «No» в поле «Cost Count».
Приоритет (Piority)
Настраиваемый диапазон: 0 ~ 255 с шагом 16.
Значение по умолчанию: 128.
Функция: Настройка приоритета порта, который определяет роли порта.
Администрирование граничного порта (Admin Edge)
Опции: Non-Edge/Edge.
Значение по умолчанию: Non-Edge.
Функция: настройка порта в режим «граничный порт».
Описание: если порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, порт считается граничным. Граничный порт может быстро, без задержки, перейти из состояния блокировки в состояние пересылки. После того, как граничный порт получает пакеты BPDU, он перестает быть граничным портом.
Граничный порт автоматически (Auto Edge)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение функции обнаружения граничного порта.
Ограничение роли (Restricted Role)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: порт с ограничением роли никогда не будет выбран в качестве корневого порта, даже если ему будет предоставлен наивысший приоритет.
Ограничение TCN (Restricted TCN)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: порт с ограниченным TCN не будет активно отправлять сообщения TCN.
Защита от BPDU (BPDU Guard)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: режим контроля перехода граничного порта в отключенное состояние из-за получения ошибок и перезагрузку при приеме пакетов BPDU.

Режим точка-точка (Point-to-point)
Опции: Auto/Forced True/Forced False.
Значение по умолчанию: Auto.
Функция: настройка типа подключения для порта. Если порт подключен к каналу «точка-точка», порт может быстро перейти в другое состояние.
Описание: «Auto» означает, что коммутатор автоматически определяет тип линии связи на основе того, что порт работает в дуплексном режиме. Если порт работает в полнодуплексном режиме, коммутатор считает, что тип канала, подключенного к порту – «точка-точка»; если порт работает в полудуплексном режиме, коммутатор считает, что тип канала, подключенного к порту, является общим. Принудительный тип связи «точка-точка» означает, что канал, подключенный к порту, является каналом «точка-точка». А принудительный общий порт означает, что канал, подключенный к порту, является общим каналом.

18.4.6. Пример типовой настройки

Как показано на рисунке 229, приоритеты коммутаторов A, B, C имеют значения 0, 4096, 8192 соответственно, а стоимость пути (path cost) трех связей имеет значения 4, 5, и 10 соответственно.

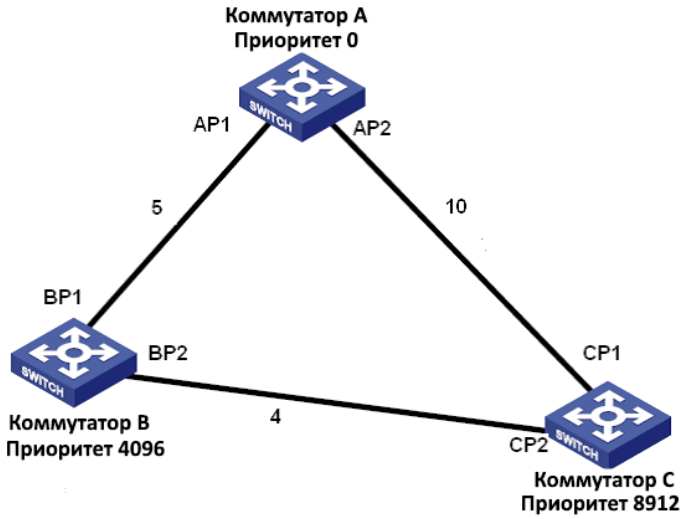


Рис. 226. Пример настройки RSTP

Настройка коммутатора A:
1. Установите значение приоритета «0», а временные параметры в значение «по умолчанию» (см. рис. 224).
2. Присвойте стоимости пути порта 1 значение 5, а стоимости пути порта 2 значение 10 (см. рис. 225).

Настройка коммутатора B:
1. Установите значение приоритета «4096», а временные параметры в значение «по умолчанию» (см. рис. 224).

2. Присвойте стоимости пути порта 1 значение 5, а стоимости пути порта 2 значение 4 (см. рис. 225).

Настройка коммутатора C:

1. Установите значение приоритета «8192», а временные параметры в значение «по умолчанию» (см. рис. 224).
2. Присвойте стоимости пути порта 1 значение 10, а стоимости пути порта 2 значение 4 (см. рис. 225).

- Приоритет коммутатора A равен «0» и имеет наименьший идентификатор, поэтому он является корневым мостом.
- Стоимость пути от AP1 до BP1 равна 5, а стоимость пути от AP2 до BP2 равна 14, поэтому BP1 является корневым портом.
- Стоимость пути от AP1 до CP2 равна 9, а стоимость пути от AP2 до CP1 равна 10, поэтому CP2 он является корневым портом, а BP2 – портом назначения.

18.5. Настройка MSTP

18.5.1. Введение

Хотя протокол RSTP обеспечивает достаточно быструю сходимость, он имеет такой же недостаток, как и STP: все мосты в локальной сети используют одно связующее дерево, и пакеты всех VLAN пересылаются по связующему дереву. Как показано на Рис. 227, определенные конфигурации могут блокировать связь между коммутатором A и коммутатором C. Поскольку коммутатор B и коммутатор D не входят в VLAN 1, они не могут пересылать пакеты VLAN 1. В результате порт VLAN 1 коммутатора A не может связываться с коммутатором C.

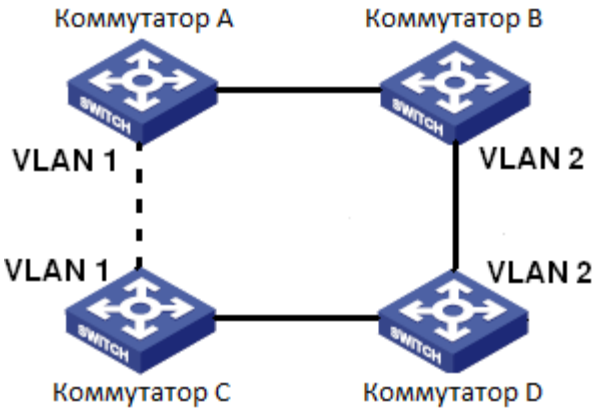


Рис. 227. Недостаток RSTP

Чтобы решить эту проблему, появился протокол MSTP. Он предоставляет как быструю конвергенцию, так и отдельные пути пересылки трафика разных VLAN для обеспечения лучшего механизма распределения нагрузки для каналов резервирования.

MSTP группирует одну или несколько VLAN в один инстанс. Коммутаторы с одинаковой конфигурацией образуют так называемый «Регион». Каждый «Регион» содержит несколько взаимно независимых связующих деревьев. «Регион» служит коммутационным

узлом. Он участвует в вычислениях с другими «Регионами» на основе алгоритма связующего дерева, вычисляя общее связующее дерево. На основе этого алгоритма сеть на рис. 227 образует топологию, показанную на рис. 228. Коммутаторы A и C находятся в Регионе 1. Ни канал связи не заблокирован, потому что в регионе отсутствуют петли. Ситуация аналогична и для Региона 2 . Регион 1 и Регион 2 аналогичны коммутационным узлам. Эти два «коммутатора» образуют петлю. Следовательно, линия связи должна быть заблокирована.

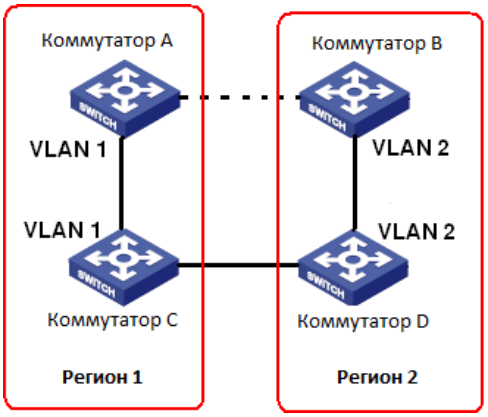


Рис. 228. Топология MSTP

18.5.2. Концепция

Концепция работы MSTP отображена на рис. 229-232.

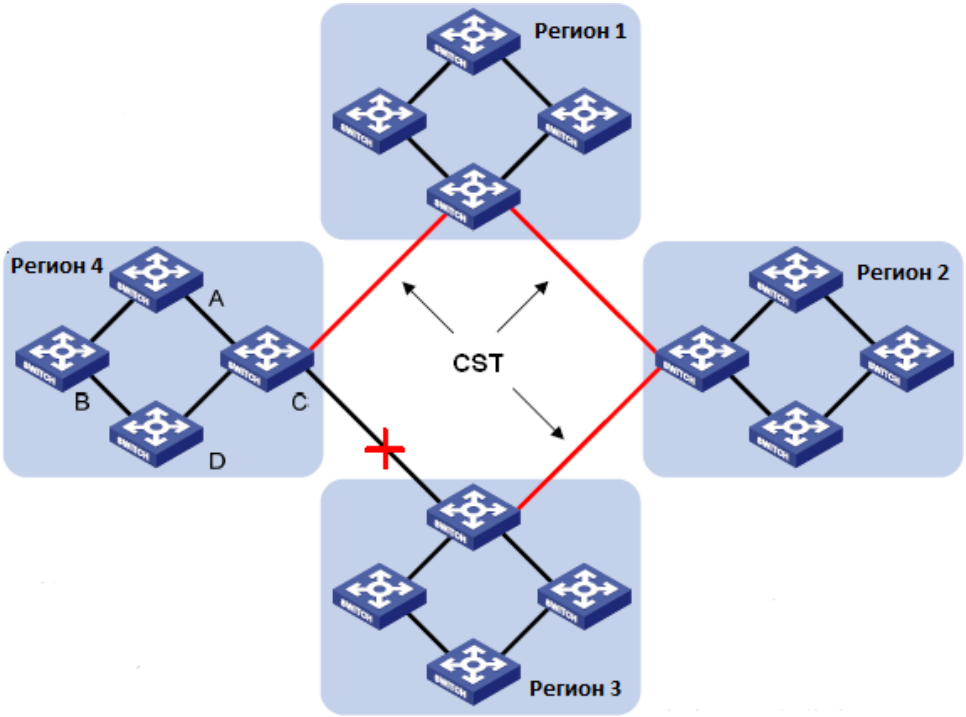


Рис. 229. Концепция MSTP

Рис. 230. Сопоставление VLAN 1 к Инстансу 1

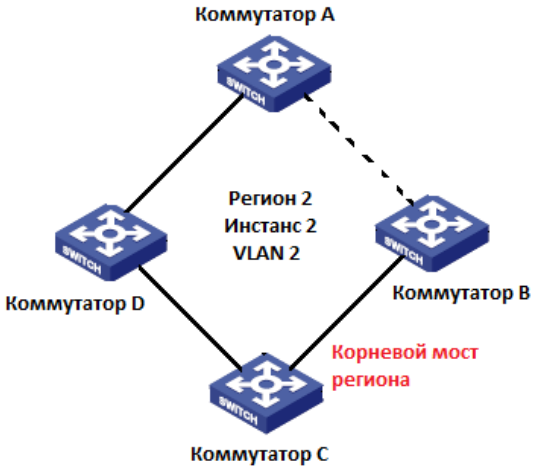


Рис. 231. Сопоставление VLAN 2 к Инстансу 2

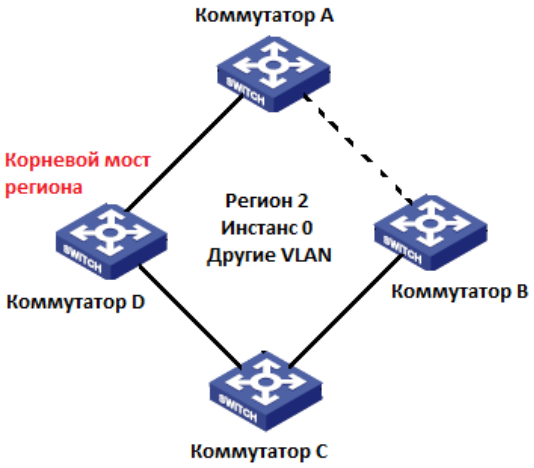


Рис. 232. Сопоставление других VLAN к Инстансу 0

Инстанс: набор из нескольких VLAN. Одна VLAN (см. рис. 230 и 231) или несколько VLAN с одинаковой топологией (см. рис. 232) могут быть сопоставлены с одним инстансом; то есть одна VLAN может сформировать связующее дерево, а несколько VLAN могут совместно использовать одно связующее дерево. Разные инстансы сопоставляются с разными связующими деревьями. Инстанс 0 - это связующее дерево для устройств всех регионов, а другие инстансы - это связующие деревья для устройств определенного региона.

Регион MST (Multiple Spanning Tree Region): коммутаторы с одинаковым именем региона MSTP, уровнем версии и сопоставлением VLAN-инстанс находятся в одом регионе MST. Как показано на рисунке 229, Регион 1, Регион 2, Регион 3 и Регион 4 - это четыре разных региона MST.

Таблица сопоставления VLAN: состоит из сопоставления между VLAN и связующими деревьями. На рис. 229 таблица сопоставления VLAN региона 2 - это сопоставление между VLAN 1 и инстансом 1, как показано на рис. 230; VLAN 2 сопоставлена с инстансом 2, как показано на рис. 231. Другие VLAN сопоставлены с инстансом 0, как показано на рис. 232.

Связующее дерево CIST (Common and Internal Spanning Tree / Общее и внутреннее связующее дерево): означает инстанс 0, то есть связующее дерево, охватывающее все устройства в сети. Как показано на рис. 229, CIST состоит из IST и CST.

Внутреннее связующее дерево (IST): означает сегмент CIST в области MST, то есть инстанс 0 для каждого региона, как показано на рис. 232.

Общее связующее дерево (CST): означает связующее дерево, соединяющее все регионы MST в сети. Если каждый регион MST является узлом, CST - это связующее дерево, вычисленное этими узлами на основе STP/RSTP. Красные линии обозначают связующее дерево (см. рис. 229).

MSTI (Multiple Spanning Tree Instance / Несколько экземпляров связующего дерева): один регион MST может образовывать несколько связующих деревьев, и они не зависят друг от друга. Каждое связующее дерево является MSTI (см. рис. 230 и Рис. 231). IST также является специальным MSTI.

Common root: означает корневой мост CIST. Коммутатор с наименьшим идентификатором корневого моста в сети является общим корневым коммутатором.

В регионе MST связующие деревья имеют разную топологию и их корневые мосты также могут быть разными. Как показано на рис. 230, 231 и 232, у этих трех инстансов разные региональные корневые мосты. Корневой мост MSTI рассчитывается на основе STP/RSTP в текущем регионе MST. Корневой мост IST - это устройство, которое подключено к другому региону MST и выбирается на основе полученной информации о приоритете.

Граничный порт (Boundary port): означает порт, который соединяет регион MST с другим регионом MST, регионом работы STP или регионом работы RSTP.

Состояние порта (Port state): порт может находиться в любом из следующих состояний в зависимости от того, изучает ли он MAC-адреса и пересылает трафик.

- Статус пересылки (Forwarding state): означает, что порт изучает MAC-адреса и выполняет пересылку пакетов.
- Статус обучения (Learning state): означает, что порт изучает MAC-адреса, но не осуществляет пересылку пакетов.

- Статус отбрасывания (Discarding state): означает, что порт не изучает MAC-адреса и не осуществляет пересылку пакетов.

Корневой порт (Root port): это наилучший порт подключения некорневого моста к корневому мосту, то есть порт с наименьшими затратами для корневого моста. Некорневой мост взаимодействует с корневым мостом именно через корневой порт. Некорневой мост имеет только один корневой порт, при этом у корневого моста нет корневого порта. Корневой порт может находиться в состоянии пересылки, обучения или отбрасывания.

Порт назначения (Designated port): порт для пересылки пакетов BPDU на другие устройства или локальные сети. Все порты корневого моста являются портами назначения. Порт назначения может находиться в состоянии пересылки, обучения или отбрасывания.

Главный порт (Master port): порт, который соединяет регион MST с общим корневым мостом и имеет к нему кратчайший путь. Исходя из CST, главный порт - это корневой порт региона (как узел). Главный порт - это специальный граничный порт. Это корневой порт для CIST и главный порт для других инстансов. Главный порт может находиться в состоянии пересылки, обучения или отбрасывания.

Альтернативный порт (Alternate port): это резервный порт для корневого порта или главного порта. При выходе из строя корневого порта или главного порта альтернативный порт становится новым корневым портом или главным портом. Альтернативный порт может находиться только в состоянии отбрасывания.

Резервный порт (Backup port): это резервный порт для порта назначения. Если порт назначения выходит из строя, резервный порт становится портом назначения и пересылает данные без каких-либо задержек. Резервный порт может находиться только в состоянии отбрасывания.

18.5.3. Реализация MSTP

MSTP делит сеть на несколько регионов MST. CST рассчитывается между регионами. В регионе вычисляется несколько связующих деревьев. Каждое связующее дерево - это MSTI. Инстанс 0 - это IST, а другие инстансы - это MSTI.

1. Расчет CIST

- Устройство отправляет и принимает пакеты BPDU. На основе сравнения пакетов с конфигурацией MSTP, устройство с наивысшим приоритетом выбирается в качестве корневого моста CIST.
- IST рассчитывается в каждом регионе MST.
- Каждый регион MST рассматривается как одно устройство, и CST рассчитывается между регионами.
- CST и IST составляют CIST всей сети.

2. Расчет MSTI

MSTP в регионе MST генерирует различные связующие деревья для VLAN на основе сопоставления VLAN и связующих деревьев. Каждое связующее дерево рассчитывается независимо. Процесс расчета аналогичен STP.

В области MST пакеты VLAN пересылаются по соответствующим MSTI. Между регионами MST пакеты VLAN пересылаются по CST.

18.5.4. Настройка через WEB-интерфейс

1. Настройка параметров сетевого моста.

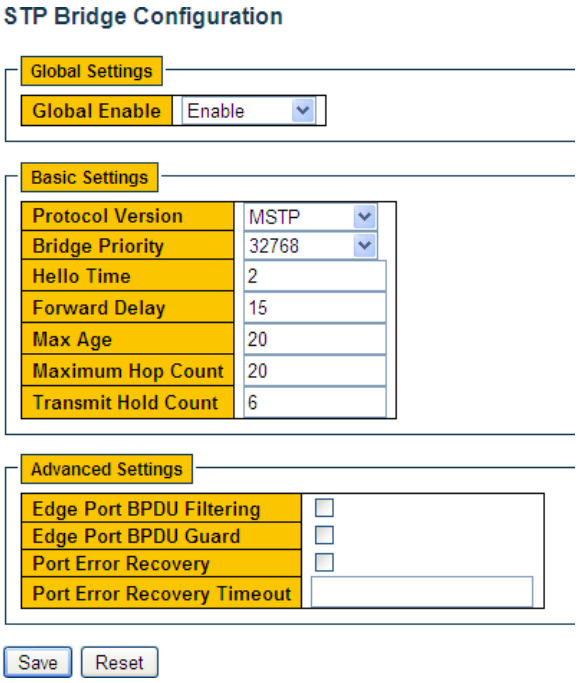


Рис. 233. Настройка параметров сетевого моста

Глобальное включение (Global Enable)

Опции: Enabled/Disabled (Включено/Выключено).

Значение по умолчанию: Disabled (Выключено).

Функция: глобальное включение и выключение STP.

- Кольцевые протоколы на основе портов включают RSTP, Sy2-Ring-Port и Sy2-RP-Port, а кольцевые протоколы на основе VLAN включают MSTP, Sy2-Ring-VLAN и Sy2-RP-VLAN.
- Кольцевые протоколы на основе портов и на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только один режим кольцевого протокола.

Приоритет протокола (MSTP/RSTP/STP)

Опции: MSTP/RSTP/STP.

Значение по умолчанию: MSTP.

Функция: выбор протокола.

Приоритет моста (Brigde Priority)

Настраиваемый диапазон: 0 ~ 61440 с шагом 4096.

Значение по умолчанию: 32768.

Функция: настройка приоритета сетевого моста
Описание: приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.

Интервал времени Hello (Hello Time)
Настраиваемый диапазон: 1 ~ 10 сек.
Значение по умолчанию: 2 сек.
Функция: Настройка временного интервала отправки настроек BPDU.

Время задержки (Forward Delay)
Настраиваемый диапазон: 4 ~ 30 сек.
Значение по умолчанию: 15 сек.
Функция: время изменения статуса от Отбрасывания (Discarding) до Изучения (Learning) и от Изучения (Learning) до Пересылки (Forwarding).

Максимальное возраст или время старения (Max Age)
Настраиваемый диапазон: 6 ~ 40 сек.
Значение по умолчанию: 20 сек.
Функция: максимальная продолжительность, в течение которой BPDU может быть сохранен на устройстве.
Описание: Если значение возраста сообщения в BPDU больше указанного значения, тогда BPDU отбрасывается.

- Значения Forward Delay Time, Hello Time и Max Age Time должны соответствовать следующим требованиям: 2 * (Forward Delay Time – 1 сек.) > = Max Age Time; Максимальное время возраста > = 2 * (время приветствия + 1 сек.).
- Рекомендуется настройка по умолчанию.

Счетчик максимального количества хопов (Maximum Hop Count)
Настраиваемый диапазон: 6 ~ 40.
Значение по умолчанию: 20.
Функция: настройка максимального количества хопов для региона MST. Максимальное количество хопов региона MST ограничивают масштаб региона MST; максимальное количество хопов для регионального корневого моста - это максимальное количество хопов региона MST.
Описание: начиная с корневого моста связующего дерева в регионе MST из числа хопов вычитается 1, когда пакет BPDU проходит через устройство в регионе. Устройство отбрасывает BPDU с номером хопа 0.

- Действительна конфигурация только с максимальным количеством хопов корневого моста в регионе MST. Устройство, не являющее корневым, использует конфигурацию хопов корневого моста.
- Рекомендуются настройки по умолчанию.

Счетчик задержки передачи (Transmit Hold Count)
Настраиваемый диапазон: 1 ~ 10.
Значение по умолчанию: 6.

Функция: настройка максимального количества пакетов BPDU, которые могут быть отправлены портом в течение каждого интервала «Hello».

Фильтрация BPDU на граничном порту (Edge Port BPDU Filtering)

Опции: Enabled/Disabled (Включено/Выключено).

Значение по умолчанию: Disabled (Выключено).

Функция: включение и выключения режима получения и отправки граничным портом пакетов BPDU.

Защита от BPDU на граничном порту (Edge Port BPDU Guard)

Опции: Enabled/Disabled (Включено/Выключено).

Значение по умолчанию: Disabled (Выключено).

Функция: режим контроля перехода граничного порта в отключенное состояние из-за получения ошибок и перезагрузку при приеме пакетов BPDU.

Восстановление порта (Port Error Recovery)

Опции: Enabled/Disabled (Включено/Выключено).

Значение по умолчанию: Disabled (Выключено).

Функция: включение или выключение режима автоматического восстановления порта из состояния ошибки в нормальное состояние.

Тайм-аут восстановления порта (Port Error Recovery Timeout)

Настраиваемый диапазон: 30 ~ 86400 сек.

Функция: настройка времени восстановления порта из состояния ошибки до нормального состояния.

2. Настройка сопоставления MSTI

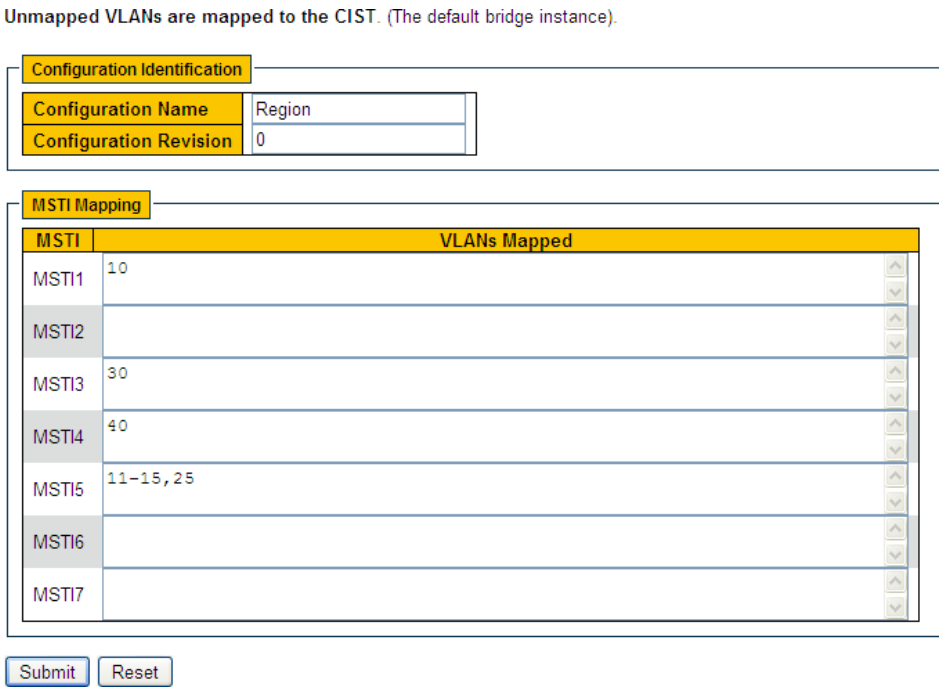


Рис. 234. Настройка сопоставления MSTI

Имя конфигурации (Configuration Name)
Настраиваемый диапазон: 1 ~ 32 символов.
Значение по умолчанию: MAC-адрес устройства.
Функция: настройка имени региона MST.
Версия конфигурации (Configuration Revision)
Настраиваемый диапазон: 0 ~ 65535.
Значение по умолчанию: 0.
Функция: настройка версии региона MST.
Описание: Параметры «версия», «имя региона» и «таблица сопоставления VLAN» определяют регион MST, к которому принадлежит устройство. Если все конфигурации совпадают, устройства находятся в одном регионе MST.
Сопоставление VLAN (VLANs Mapped)
Настраиваемый диапазон: 1 ~ 4094.
Функция: настройка таблицы сопоставления VLAN в регионе MST. При наличии нескольких VLAN вы можете разделить VLAN запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая используется для разделения двух непоследовательных идентификаторов VLAN.
Описание: по умолчанию все VLAN сопоставляются с инстансом 0. Одна VLAN сопоставляется только с одним инстансом связующего дерева. Если VLAN сопоставляется с другим инстансом, предыдущее сопоставление отменяется. Если сопоставление между указанной VLAN и инстансом было удалено, эта VLAN будет сопоставлена с инстансом 0.

3. Настройка приоритета моста для коммутатора в удаленном инстансе.

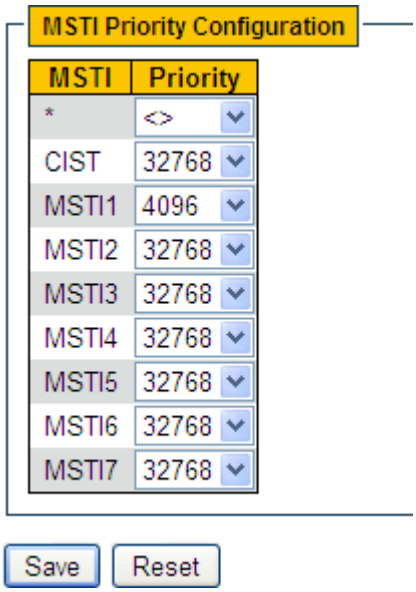


Рис. 235. Настройка приоритета моста

Приоритет (Priority)
Настраиваемый диапазон: 0 ~ 61440 с шагом 4096.

Значение по умолчанию: 32768.
Функция: настройка приоритета моста для коммутатора в удаленном инстансе.
Описание: приоритет моста определяет, может ли коммутатор быть выбран в качестве регионального корневого моста для инстанса связующего дерева. Чем меньше значение, тем выше приоритет. Установив более низкий приоритет, данное устройство может быть назначено корневым мостом связующего дерева. Устройство с поддержкой MSTP можно настроить с разными приоритетами в разных инстансах связующего дерева.

Нажмите <Save>, чтобы текущие настройки вступили в силу.

4. Настройка портов CIST

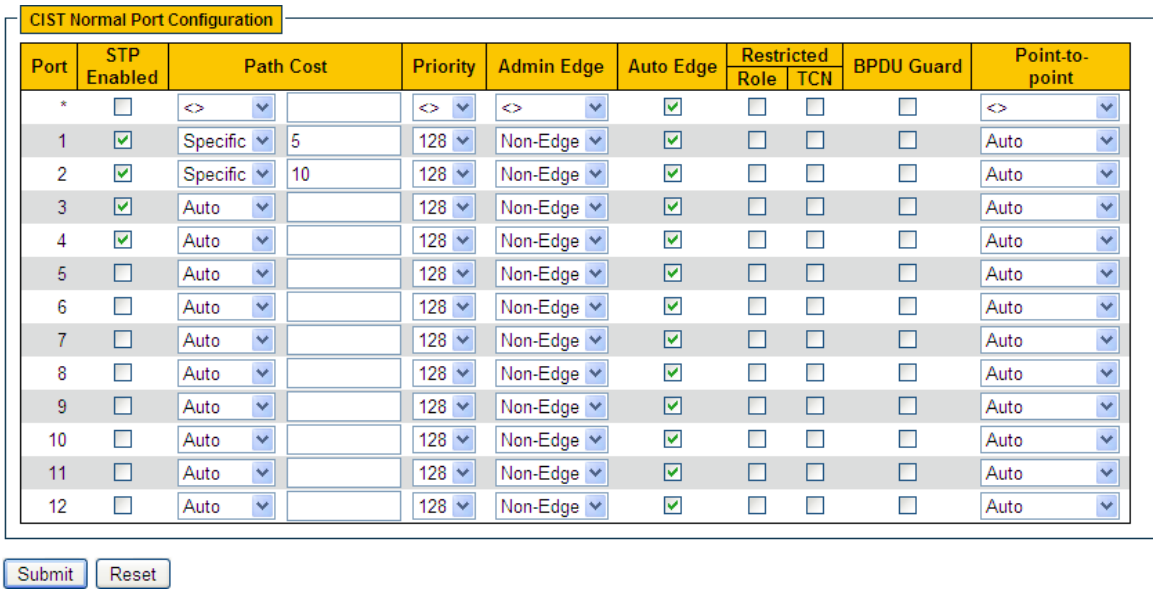


Рис. 236. Настройка портов CIST

Включение STP (STP Enabled)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение STP/RSTP на порту.

- Порт MSTP и транковый порт являются взаимоисключающими. Порт MSTP нельзя добавить к транковому порту; транковый порт не может быть настроен как порт RSTP.
- Не рекомендуется, чтобы порты в изолированной группе были одновременно настроены как порты MSTP, а порты MSTP не могут быть добавлены в изолированную группу.

Стоимость пути (Path Cost)
Настраиваемый диапазон: Auto/Specific 1 ~ 200000000.

Значение по умолчанию: Auto.
Функция: стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от пропускной способности. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение, вручную выберите «No» в поле «Cost Count».

Приоритет (Piority)

Настраиваемый диапазон: 0 ~ 240 с шагом 16
Значение по умолчанию: 128
Функция: настройка приоритета порта, который определяет роли порта.

Администрирование граничного порта (Admin Edge)

Опции: Non-Edge/Edge.
Значение по умолчанию: Non-Edge.
Функция: настройка порта в режим «граничный порт».
Описание: если порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, порт считается граничным. Граничный порт может быстро, без задержки, перейти из состояния блокировки в состояние пересылки. После того, как граничный порт получает пакеты BPDU, он перестает быть граничным портом.

Граничный порт автоматически (Auto Edge)

Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение функции обнаружения граничного порта.

Ограничение роли (Restricted Role)

Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: порт с ограничением роли никогда не будет выбран в качестве корневого порта, даже если ему будет предоставлен наивысший приоритет.

Ограничение TCN (Restricted TCN)

Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: порт с ограниченным TCN не будет активно отправлять сообщения TCN.

Защита от BPDU (BPDU Guard)

Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: режим контроля перехода граничного порта в отключенное состояние из-за получения ошибок и перезагрузку при приеме пакетов BPDU.

Режим точка-точка (Point-to-point)

Опции: Auto/Forced True/Forced False.
Значение по умолчанию: Auto.
Функция: настройка типа подключения для порта. Если порт подключен к каналу «точка-точка», порт может быстро перейти в другое состояние.
Описание: «Auto» означает, что коммутатор автоматически определяет тип линии связи на основе того, что порт работает в дуплексном режиме. Если порт работает в

полнодуплексном режиме, коммутатор считает, что тип канала, подключенного к порту – «точка-точка»; если порт работает в полудуплексном режиме, коммутатор считает, что тип канала, подключенного к порту, является общим. Принудительный тип связи «точка-точка» означает, что канал, подключенный к порту, является каналом «точка-точка». А принудительный общий порт означает, что канал, подключенный к порту, является общим каналом.

5. Настройка портов MSTI.

Рис. 237. Выбор MSTI

Выбор MSTI (Select MSTI)
Настраиваемый диапазон: MST1~MST7
Значение по умолчанию: MST1
Функция: выберите MSTI, нажмите <Get>, чтобы перейти на страницу настройки портов MSTI, как показано на следующем рис. 238.

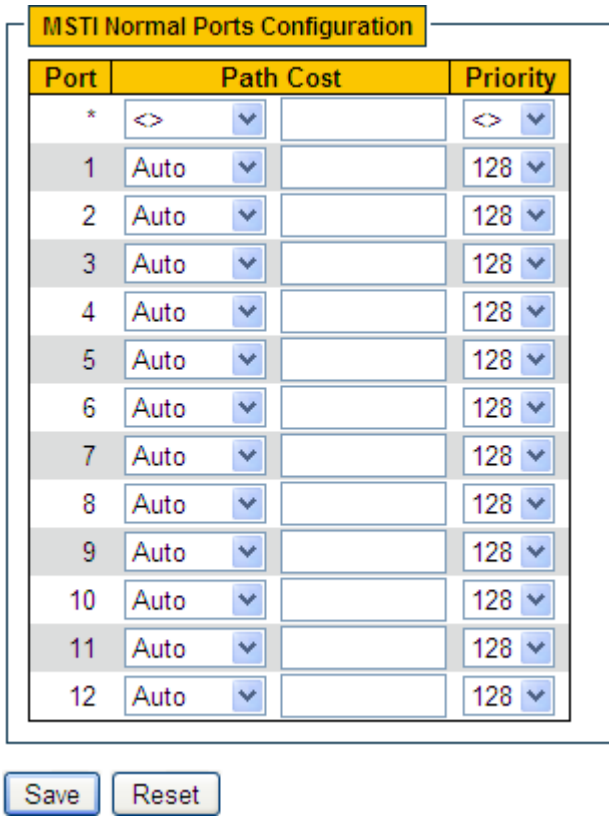


Рис. 238. Настройка портов MSTI

Стоимость пути (Path Cost)
Настраиваемый диапазон: Auto/Specific 1 ~ 200000000.
Значение по умолчанию: Auto.

Функция: настройка стоимости пути порта в инстансе назначения.
Описание: стоимость пути порта используется для расчета оптимального пути. Значение параметра зависит от пропускной способности. Чем больше значение, тем ниже стоимость. Изменение стоимости пути к порту может изменить путь передачи между устройством и корневым мостом, тем самым изменив роль порта. Порт с поддержкой MSTP может быть настроен с различной стоимостью пути в разных инстансах связующего дерева.

Приоритет (Piority)
Настраиваемый диапазон: 0 ~ 240 с шагом 16
Значение по умолчанию: 128
Функция: настройка приоритета порта в инстансе назначения.
Описание: приоритет порта определяет, будет ли он выбран корневым портом. орт с более низким приоритетом будет выбран корневым портом. Порты с поддержкой MSTP могут быть настроены с разными приоритетами и играть разные роли в разных инстансах связующего дерева.

6. Просмотр статуса моста.

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-01-C1-00-00-00	32768.00-01-C1-00-00-00	-	0	Steady	-
MSTI1	32769.00-01-C1-00-00-00	32769.00-01-C1-00-00-00	-	0	Steady	-
MSTI3	32771.00-01-C1-00-00-00	32771.00-01-C1-00-00-00	-	0	Steady	-
MSTI4	32772.00-01-C1-00-00-00	32772.00-01-C1-00-00-00	-	0	Steady	-
MSTI5	32773.00-01-C1-00-00-00	32773.00-01-C1-00-00-00	-	0	Steady	-

Рис. 239. Отображение статуса моста

7. Просмотр статуса порта STP.

STP Port Status

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 01:03:13
2	DesignatedPort	Forwarding	0d 00:03:32
3	BackupPort	Discarding	0d 00:03:32
4	Disabled	Discarding	-
5	Non-STP	Discarding	-
6	Non-STP	Discarding	-
7	Non-STP	Discarding	-
8	Non-STP	Discarding	-
9	Non-STP	Discarding	-
10	Non-STP	Discarding	-
11	Non-STP	Discarding	-
12	Non-STP	Discarding	-

Рис. 240. Отображение статуса порта STP

8. Просмотр статистики пакетов порта STP.

STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	1960	1180	0	0	0	0	0	0	0	0
2	164	0	0	0	3	0	0	0	0	0
3	3	0	0	0	164	0	0	0	0	0

Рис. 241. Отображение статистики пакетов порта STP

18.5.5. Пример типовой настройки

Как показано на Рис. 241, коммутаторы A, B, C и D принадлежат одному и тому же региону MST. VLAN, отмеченные красным, означают, что пакеты VLAN могут быть переданы по каналам связи. После завершения настройки пакеты VLAN можно пересылать по разным инстансам связующего дерева. Пакеты VLAN 10 пересылаются по инстансу 1, а корневым мостом инстанса 1 является коммутатор A. Пакеты VLAN 30 пересылаются по инстансу 3, а корневой мост инстанса 3 - это коммутатор B. Пакеты VLAN 40 пересылаются по инстансу 4, а корневой мост инстанса 4 - это коммутатор C. Пакеты VLAN 20 пересылаются по инстансу 0, а корневым мостом инстанса 0 является коммутатор B.

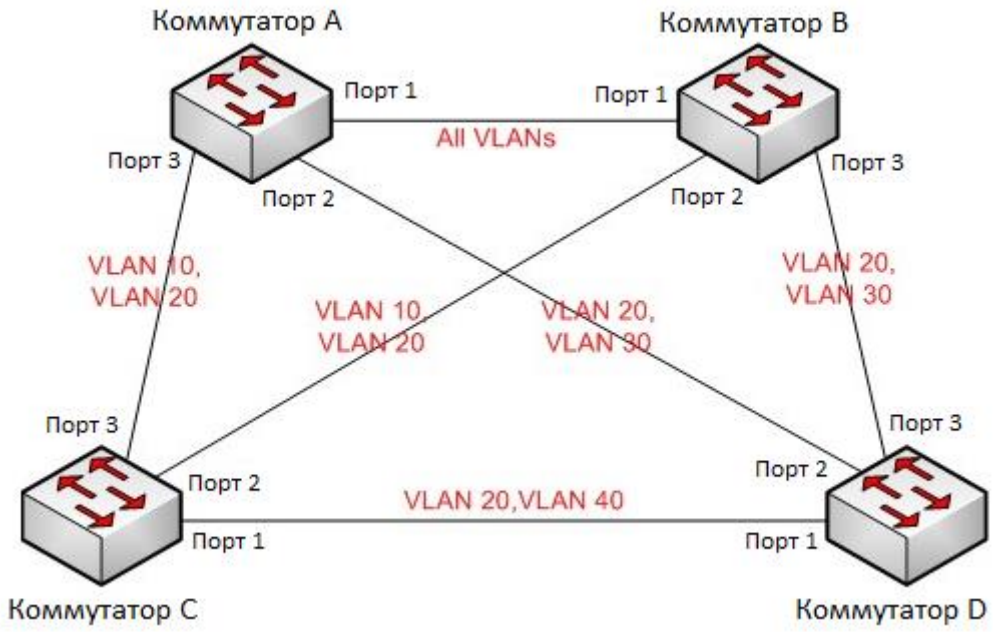


Рис. 242. Пример типовой настройки MSTP

Настройка коммутатора A:

1. Создайте VLAN 10, 20 и 30 на коммутаторе A; на портах установите разрешение на прохождение пакетов соответствующих VLAN.
2. Включите глобальный протокол MSTP (см. рис. 233).

3. Задайте для имени региона MST значение «Region», а для параметра «Revision» - 0 (см. рис. 234).
4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с инстансами 1, 3 и 4 соответственно (см. рис. 234).
5. Установите приоритет моста коммутатора в MSTI 1 на 4096 и сохраните приоритет по умолчанию в других инстансах (см. рис. 235).

Настройка коммутатора B:

1. Создайте VLAN 10, 20 и 30 на коммутаторе B; на портах установите разрешение на прохождение пакетов соответствующих VLAN.
2. Включите глобальный протокол MSTP (см. рис. 233).
3. Задайте для имени региона MST значение «Region», а для параметра «Revision» - 0 (см. рис. 234).
4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с инстансами 1, 3 и 4 соответственно (см. рис. 234).
5. Установите приоритет моста коммутатора в MSTI 3 и MSTI 0 на 4096 и сохраните приоритет по умолчанию в других инстансах (см. рис. 235).

Настройка коммутатора C:

1. Создайте VLAN 10, 20 и 40 на коммутаторе C; на портах установите разрешение на прохождение пакетов соответствующих VLAN.
2. Включите глобальный протокол MSTP (см. рис. 233).
3. Задайте для имени региона MST значение «Region», а для параметра «Revision» - 0 (см. рис. 234).
4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с инстансами 1, 3 и 4 соответственно (см. рис. 234).
5. Установите приоритет моста коммутатора в MSTI 4 на 4096 и сохраните приоритет по умолчанию в других инстансах (см. рис. 235).

Настройка коммутатора C:

1. Создайте VLAN 20, 30 и 40 на коммутаторе D; на портах установите разрешение на прохождение пакетов соответствующих VLAN.
2. Включите глобальный протокол MSTP (см. рис. 233).
3. Задайте для имени региона MST значение «Region», а для параметра «Revision» - 0 (см. рис. 234).
4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с инстансами 1, 3 и 4 соответственно (см. рис. 234).

Когда расчет MSTP завершен, MSTI каждой VLAN выглядит следующим образом:

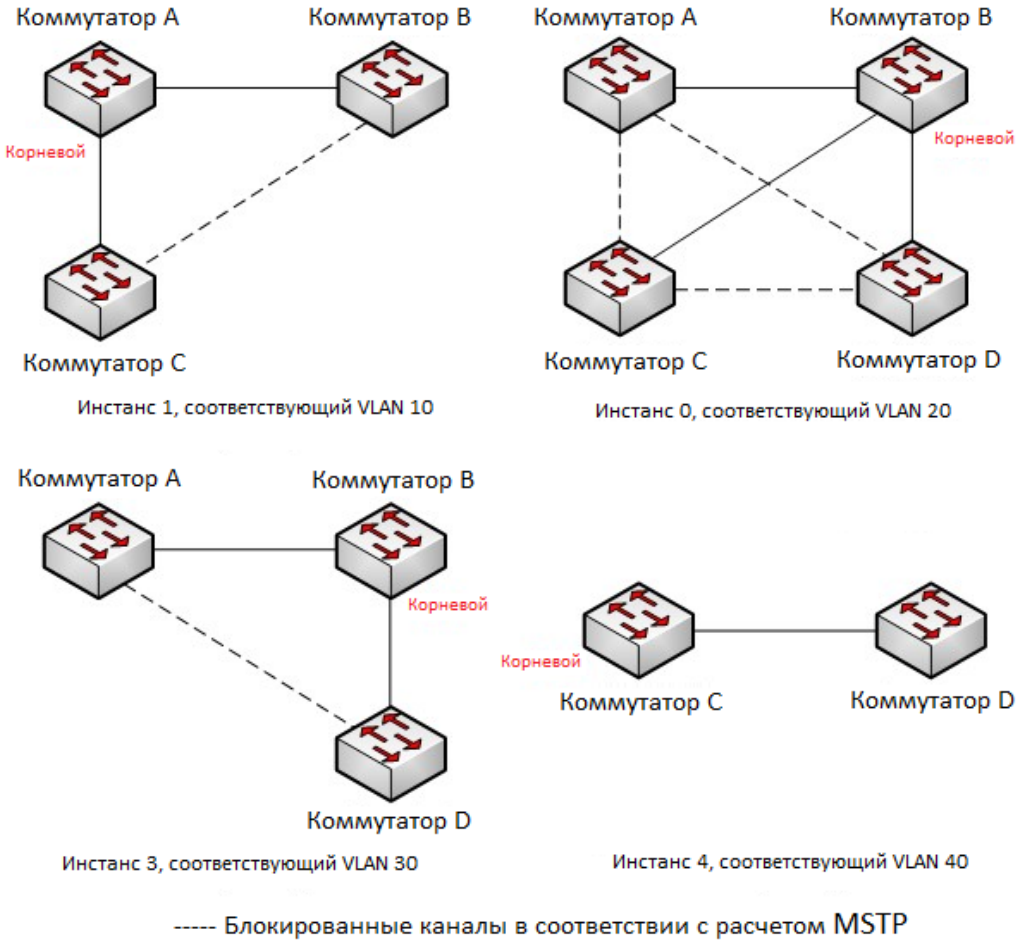


Рис. 243. Инстансы связующего дерева для каждой VLAN

19. Аварийная сигнализация (Alarm)

19.1. Введение

Данная серия коммутаторов поддерживает следующие типы аварийной сигнализации:

- Аварийная сигнализация электропитания (Power alarm): если включена данная функция, аварийная сигнализация будет срабатывать в случае проблем с одним из источников электропитания;
- Аварийная сигнализация использования Памяти/ЦП (Memory/CPU Usage Alarm): если эта функция включена, аварийная сигнализация срабатывает, когда использование Памяти/ЦП превышает указанный порог.
- Аварийная сигнализация при конфликте IP и/или MAC адресов (IP/MAC conflict alarm): если данная функция включена, аварийная сигнализация будет срабатывать в случае, если в сети будут обнаружены одинаковые IP и/или MAC адреса;
- Аварийная сигнализация на порту (Port alarm): если включена данная функция, аварийная сигнализация будет срабатывать в случае получении информации об отключении соответствующего порта (состояние Link Down).

- Аварийная сигнализация кольца (Ring alarm): если включена данная функция, аварийная сигнализация будет срабатывать в случае нарушения кольцевой топологии, т.е. размыкании кольца.
- Аварийная сигнализация CRC и потери пакетов (CRC and Packet Loss alarm): если эта функция включена, аварийная сигнализация будет срабатывать, когда количество ошибок CRC/потери пакетов на порту превышает указанный порог.
- Аварийная сигнализация по скорости порта (Port Rate Alarm): если эта функция включена, аварийная сигнализация будет срабатывать, когда скорость входящего/исходящего трафика порта превышает указанный порог.
- Аварийная сигнализация для модуля SFP.

Функцию аварийной сигнализации кольца (Ring alarm) поддерживают только Мастер кольца Sy2-Ring и корневой коммутатор Sy2-RP.

19.2. Настройка через WEB-интерфейс

1. Настройка и отображение аварийных сигналов по питанию и использованию памяти/CPU.

Alarm Configuration

Alarm Type	Enable	Threshold		Margin Value		Status
Power Alarm	☑	---		---		Power-1:Power Down | Power-2:Power On
Mem Usage Alarm	☑	85	(50~100)	5	(1~20)	Normal
CPU Usage Alarm	☑	85	(50~100)	5	(1~20)	Normal

Рис. 244. Настройка аварийной сигнализации

Аварийная сигнализация питания (Power Alarm)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение аварийной сигнализации электропитания.
Статус (Status)
Опции: Power On/Power Down (Питание включено/Питание выключено).
Описание: «Power On» означает, что питание подключено и работает нормально. «Power Down» означает, что питание отключено или работает со сбоями.
Аварийная сигнализация Памяти/ЦП (Mem/CPU Usage Alarm)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение аварийной сигнализации, сообщающей об ошибках памяти или ЦП.
Пороговое значение (Threshold (%))
Настраиваемый диапазон: 50 ~ 100.
Значение по умолчанию: 85.

Функция: настройка порога использования памяти/ЦП. Когда использование памяти/ЦП коммутатора превышает пороговое значение, генерируется аварийный сигнал.

Допустимое отклонение от порогового значения (Margin Value (%))

Настраиваемый диапазон: 50 ~ 100.

Значение по умолчанию: 85.

Функция: настройка значения допустимого отклонения от порогового значения использования памяти/ЦП.

Описание: если использование памяти/ЦП колеблется около порогового значения, сигналы тревоги могут повторно генерироваться и сбрасываться. Чтобы предотвратить это явление, вы можете указать значение допустимого отклонения порогового значения (по умолчанию 5%). Аварийный сигнал будет сброшен только в том случае, если использование памяти /ЦП ниже порогового значения на величину запаса или больше. Например, порог использования памяти установлен на 60%, а значение допустимого отклонения установлено на 5%. Если использование памяти коммутатора меньше или равно 60%, сигнал тревоги не генерируется. Если использование памяти превышает 60%, будет сгенерирован сигнал тревоги. Аварийный сигнал будет сброшен только в том случае, если использование памяти равно или меньше 55%.

Статус аварийной сигнализации (Alarm Status)

Опции: Normal /Alarm.

Описание: отображение состояния использования памяти/ЦП коммутатора. «Alarm» означает, что использование памяти/ЦП превышает пороговое значение.

2. Настройка и отображение аварийной сигнализации при конфликте IP и/или MAC адресов.

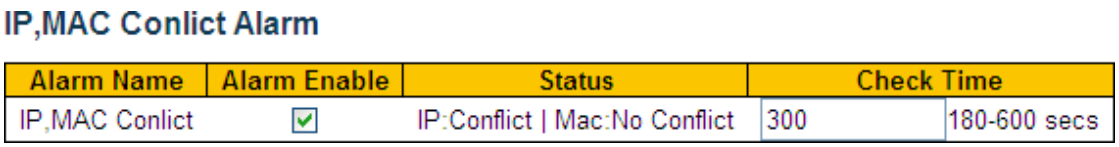


Рис. 245. Настройка аварийной сигнализации при конфликте IP и/или MAC адресов

Аварийная сигнализация конфликта IP и MAC адресов (IP, MAC Conflict)

Опции: Enabled/Disabled (Включено/Выключено).

Значение по умолчанию: Disabled (Выключено).

Функция: включение и выключение аварийной сигнализации при конфликте IP и/или MAC адресов.

Статус (Status)

Опции: Conflict/No Conflict (Есть конфликт/Нет конфликта).

Описание: если возникает конфликт IP/MAC адресов, отображается «Conflict»; в противном случае отображается «No Conflict».

Пороговое значение (Check Time)

Настраиваемый диапазон: 180 ~ 600 сек.

Значение по умолчанию: 300 сек.

Функция: настройка интервала обнаружения конфликтов IP/MAC адресов.

3. Настройка и отображение аварийной сигнализации Sy2-Ring.

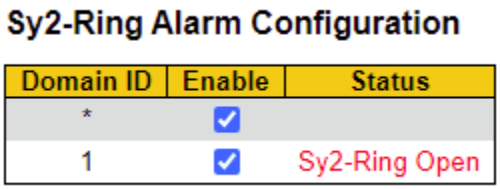


Рис. 246. Настройка аварийной сигнализации Sy2-Ring

Аварийная сигнализация Sy2-Ring (Sy2-Ring Alarm Configuration)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение аварийной сигнализации Sy2-Ring.
Статус (Status)
Опции: Sy2-Ring Close/Sy2-Ring Open.
Описание: «Sy2-Ring Close» означает, что кольцо замкнуто. «Sy2-Ring Open» означает, что кольцо разомкнуто или находится работает с ошибками.

4. Настройка и отображение аварийной сигнализации Sy2-RP.

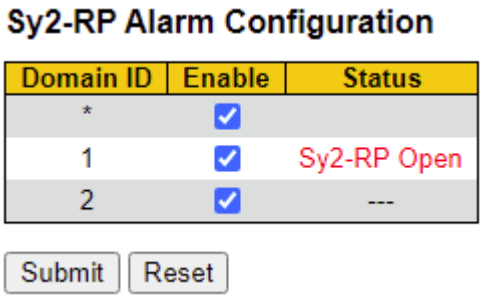


Рис. 247. Настройка аварийной сигнализации Sy2-RP

Аварийная сигнализация Sy2-RP (Sy2-RP Alarm Configuration)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение аварийной сигнализации Sy2-RP.
Статус (Status)
Опции: Sy2-RP Close/Sy2-RP Open.
Описание: «Sy2-RP Close» означает, что кольцо замкнуто. «Sy2-RP Open» означает, что кольцо разомкнуто или находится работает с ошибками.

5. Настройка и отображение аварийной сигнализации на порту.

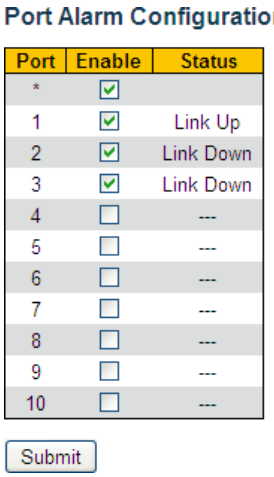


Рис. 248. Настройка аварийной сигнализации на порту

Аварийная сигнализация на порту (Port Alarm Configuration)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение аварийной сигнализации на порту.
Статус (Status)
Опции: Link Up/Link Down.
Описание: «Link Up» означает, что порт находится в состоянии подключения и обеспечивает нормальную связь. «Link Down» означает, что порт отключен или произошел сбой связи.

6. Настройка и отображение аварийной сигнализации CRC и потери пакетов.

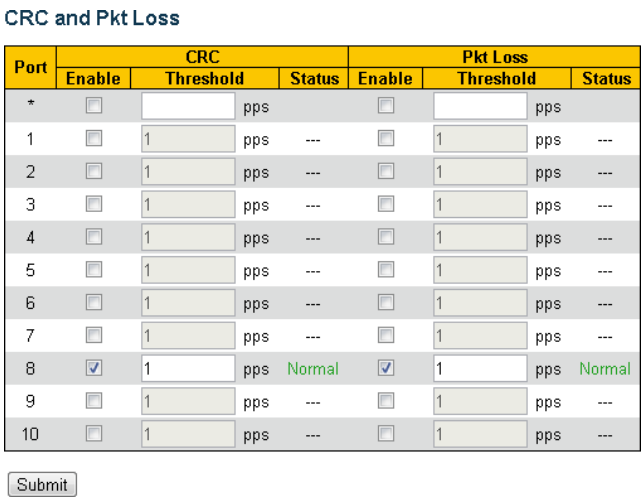


Рис. 249. Настройка аварийной сигнализации CRC и потери пакетов

Аварийная сигнализация CRC и потери пакетов (CRC/Pkt Loss Alarm)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение аварийной сигнализации CRC и потери пакетов.
Пороговое значение (Threshold)
Настраиваемый диапазон: 1 ~ 1000000 pps (пак/с).
Функция: настройка порогового значения CRC и потери пакетов на порту.
Статус (Alarm Status)
Опции: Alarm/Normal.
Описание: отображение статуса потери CRC/Пакетов на порту. «Alarm» означает, что потери CRC/Пакетов на порту превышают пороговое значение.

7. Настройка и отображение аварийной сигнализации по скорости порта.

Port Rate Alarm

Port	Input Rate Alarm				Output Rate Alarm			
	Enable	Threshold	Unit	Status	Enable	Threshold	Unit	Status
*	☐		<>		☐		<>	
1	☐	1	bps	---	☐	1	bps	---
2	☐	1	bps	---	☐	1	bps	---
3	☐	1	bps	---	☐	1	bps	---
4	☐	1	bps	---	☐	1	bps	---
5	☐	1	bps	---	☐	1	bps	---
6	☐	1	bps	---	☐	1	bps	---
7	☐	1	bps	---	☐	1	bps	---
8	☐	1	bps	---	☐	1	bps	---
9	☐	1	bps	---	☐	1	bps	---
10	☐	1	bps	---	☐	1	bps	---

Submit

Рис. 250. Настройка аварийной сигнализации по скорости порта

Аварийная сигнализация скорости входящего/исходящего трафика (input rate alarm/output rate alarm)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение аварийной сигнализации скорости входящего/исходящего трафика.
Пороговое значение (Threshold)
Настраиваемый диапазон: 1 ~ 1000000000 bps (бит/с) или 1 ~ 1000000 kbps (Кбит/с).
Функция: настройка порогового значения трафика на порту.
Статус (Alarm Status)
Опции: Alarm/Normal.
Описание: отображение статуса трафика на порту. «Alarm» означает, что скорость входящего/исходящего трафика на порту превышают пороговое значение.

8. Настройка и отображение аварийной сигнализации питания на порту RX у SFP.

Soft Alarm

Port	Enable	Threshold(-40.0~8.2)	Status
*	☐	dBm	
9	☑	-22.0 dBm	Alarm
10	☐	-22.0 dBm	---

Hard Alarm Mode

Hard Alarm Mode	Enable

Submit

Hard Alarm Status

Port	RX Power Alarm			TX Power Alarm		
	Current Value	High Alarm State	Low Alarm State	Current Value	High Alarm State	Low Alarm State
9	-40.5	Normal	Alarm	-9.6	Normal	Normal

Рис. 251. Настройка аварийной сигнализации питания на порту RX у SFP

Аварийная сигнализация по программному обеспечению (Software Alarm)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение аварийной сигнализации на порту RX у модуля SFP.
Пороговое значение (Threshold)
Настраиваемый диапазон: -40 ~ 8,2 dBm (дБм).
Значение по умолчанию: -22,0 dBm (дБм).
Функция: настройка порогового значения аварийной сигнализации на порту RX у модуля SFP.
Статус (Alarm Status)
Опции: NotSupportDDM/NotExist/Normal/Alarm.
Функция: аварийная сигнализация ПО относится к порту, принимающему аварийный сигнал. Необходимо, чтобы модуль SFP поддерживал функцию DDM. Если модуль SFP не вставлен в порт, то отображается статус «NotExist». Если модуль SFP вставлен, но при этом DDM не поддерживается, отображается статус «NotSupportDDM». Если вставлен модуль SFP с поддержкой DDM и мощность принимаемого оптического сигнала ниже порогового значения, то будет сгенерирован статус «Alarm». Если вставлен модкль SFP с поддержкой DDM и мощность принимаемого оптического сигнала не ниже порогового значения, тогда отображается статус «Normal».
Аварийная сигнализация оборудования (Hardware Alarm)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).

Функция: включение и выключение аварийной сигнализации по аппаратному обеспечению модуля SFP.

Статус (Alarm Status)
Опции: Alarm/ Normal.
Функция: отображение состояния аварийного сигнала оборудования питания SFP. Поддерживает аварийную сигнализацию питания модуля SFP на портах Tx/Rx, но порог срабатывания Tx не настраивается.

20. Проверка канала связи (Link Check)

20.1. Введение

Проверка канала связи предполагает периодический обмен информацией между специальными протоколами пакетов данных для оценки возможности соединения и отображения состояния связи на порту. При получении информации о неисправности, проблему можно вовремя обнаружить и устранить.
Порт, для которого включена проверка состояния канала, периодически (каждые 1 сек.) отправляет пакеты проверки канала связи для проверки его состояния. Если порт не получает пакет проверки канала от однорангового узла в течение периода тайм-аута (5 сек.), это указывает на то, что канал связи неисправен, а порт отображает состояние ошибки Rx. Если порт получает пакет проверки связи от однорангового узла и отображается, что пакет проверки связи получен с локального узла в течение периода тайм-аута (5 сек.), порт показывает, что он находится в работоспособном состоянии. Если порт получает пакет проверки связи от однорангового узла, но отображается, что пакет проверки связи не получен с локального узла в течение периода тайм-аута (5 сек.), порт отображает состояние ошибки Tx. Если к порту не подключен канал связи, порт отображает статус «Link down».
Порт, для которого отключена проверка статуса связи, работает в пассивном режиме. То есть он не отправляет пакет проверки связи. Однако после получения пакета проверки связи этот порт немедленно возвращает пакет проверки связи, чтобы проинформировать другую сторону о том, что он получил пакет проверки связи.

20.2. Настройка через WEB-интерфейс

1. Настройка функции проверки канала связи.

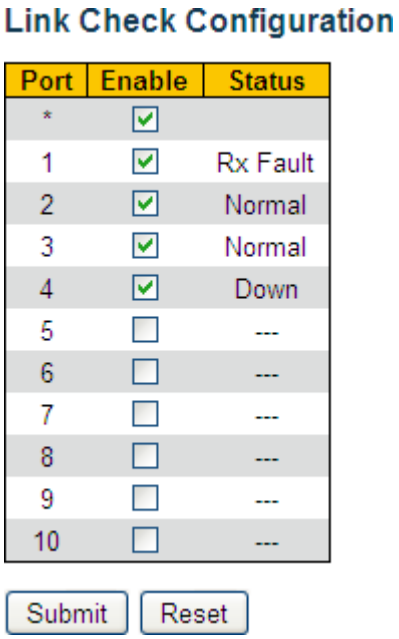


Рис. 252. Настройка функции проверки канала связи

Включение (Enable)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и выключение функции проверки канала связи.

Если одноранговое устройство не поддерживает эту функцию, она должна быть отключена на подключенном порту локального устройства.

Статус (Alarm Status)
Опции: Up/Normal/--/Rx Fault/Tx Fault/Down.
Функция: если для порта включена функция проверки связи и порт отправляет/принимает данные в обычном режиме, отображается статус «Normal». Если одноранговая сторона не получает подтверждающие пакеты от устройства, отображается статус «Tx Fault». Если устройство не получает подтверждающие пакеты от однорангового узла, отображается статус «Rx Fault». Если порт не подключен к сети, отображается стстус «Down». Если для порта не включена проверка связи, отображается статус «--». В момент подключения порта и включения функции проверки связи отображается статус «Up».

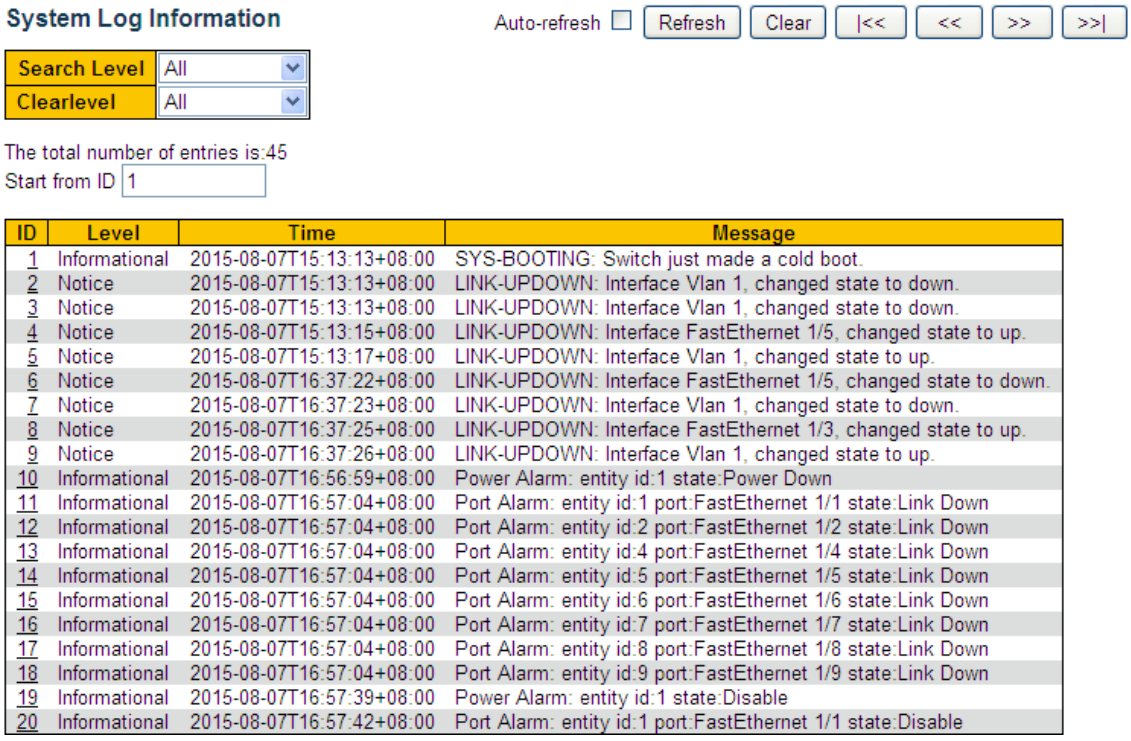
21. Системный журнал (Log)

21.1. Введение

Функция системного журнала предназначена для записи состояние системы, информацию о неисправностях и другую информацию. При соответствующей конфигурации коммутатор может выгружать файлы с записями на сервер, поддерживающий Syslog, в режиме реального времени.
Журнал содержит информацию с аварийными сообщениями, о широковещательном шторме, перезагрузке, проблемах с памятью и информацию о действиях пользователей.

21.2. Настройка через WEB-интерфейс

1. Настройка системного журнала



ID	Level	Time	Message
1	Informational	2015-08-07T15:13:13+08:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	2015-08-07T15:13:13+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	2015-08-07T15:13:13+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
4	Notice	2015-08-07T15:13:15+08:00	LINK-UPDOWN: Interface FastEthernet 1/5, changed state to up.
5	Notice	2015-08-07T15:13:17+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
6	Notice	2015-08-07T16:37:22+08:00	LINK-UPDOWN: Interface FastEthernet 1/5, changed state to down.
7	Notice	2015-08-07T16:37:23+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
8	Notice	2015-08-07T16:37:25+08:00	LINK-UPDOWN: Interface FastEthernet 1/3, changed state to up.
9	Notice	2015-08-07T16:37:26+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
10	Informational	2015-08-07T16:56:59+08:00	Power Alarm: entity id:1 state:Power Down
11	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:1 port:FastEthernet 1/1 state:Link Down
12	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:2 port:FastEthernet 1/2 state:Link Down
13	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:4 port:FastEthernet 1/4 state:Link Down
14	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:5 port:FastEthernet 1/5 state:Link Down
15	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:6 port:FastEthernet 1/6 state:Link Down
16	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:7 port:FastEthernet 1/7 state:Link Down
17	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:8 port:FastEthernet 1/8 state:Link Down
18	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:9 port:FastEthernet 1/9 state:Link Down
19	Informational	2015-08-07T16:57:39+08:00	Power Alarm: entity id:1 state:Disable
20	Informational	2015-08-07T16:57:42+08:00	Port Alarm: entity id:1 port:FastEthernet 1/1 state:Disable

Рис. 253. Настройка системного журнала

Уровень поиска (Search Level)
Опции: Error/Warning/Notice/Information/All (Ошибка/Предупреждение/Уведомление/Информация/Все).
Значение по умолчанию: All (Все).
Функция: выбор уровня отображаемой информации системного журнала.
Уровень очистки (Clear level)
Опции: Error/Warning/Notice/Information/All (Ошибка/Предупреждение/Уведомление/Информация/Все).
Значение по умолчанию: All (Все).

Функция: выбор уровня удаляемой информации системного журнала. Нажмите <Clear>, чтобы удалить информацию журнала соответствующего уровня.

Общее количество (The total number)

Функция: отображение количества журналов, удовлетворяющих условиям запроса.

Стартовый идентификатор (Start from ID)

Функция: настройка стартового идентификатора записей системного журнала на текущей странице. Вы можете нажать «Refresh», чтобы обновить записи журнала на текущей странице. На каждой странице может отображаться до 20 записей системного журнала.

Нажмите [>>], чтобы просмотреть записи журнала на следующей странице. Идентификатор начала следующей страницы - это идентификатор последней записи журнала на текущей странице.

Нажмите [<<], чтобы просмотреть записи журнала на предыдущей странице.

Нажмите [>>|], чтобы просмотреть записи системного журнала на последней странице. Конечный идентификатор - это идентификатор последней записи журнала.

Нажмите [|<<], чтобы просмотреть записи журнала на первой странице. Идентификатор начала - это идентификатор первой записи журнала.

2. Загрузка системного журнала на сервер в режиме реального времени.

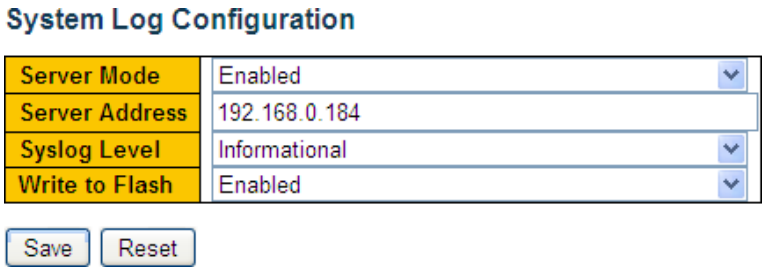


Рис. 254. Загрузка системного журнала на сервер

Режим сервера (Server Mode)

Опции: Enabled/Disabled (Включено/Выключено).

Значение по умолчанию: Disabled (Выключено).

Функция: включение и отключение режима загрузки журнала на сервер в реальном времени.

Адрес сервера (Server Address)

Функция: настройка IP-адреса сервера, на который загружается информация системного журнала.

Уровень системного журнала (Syslog Level)

Опции: Error/Warning/Notice/Information (Ошибка/Предупреждение/Уведомление/Информация).

Значение по умолчанию: Information (Информация).

Функция: выбор уровня информации системного журнала для загрузки на сервер.

Запись в память Flash (Write to Flash)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и отключение режима записи во Flash-память.

Вы можете установить программное обеспечение «Syslog Server», например «Tftp32», на ПК для создания сервера записей системного журнала.
Информация системного журнала может отображаться на сервере в режиме реального времени.

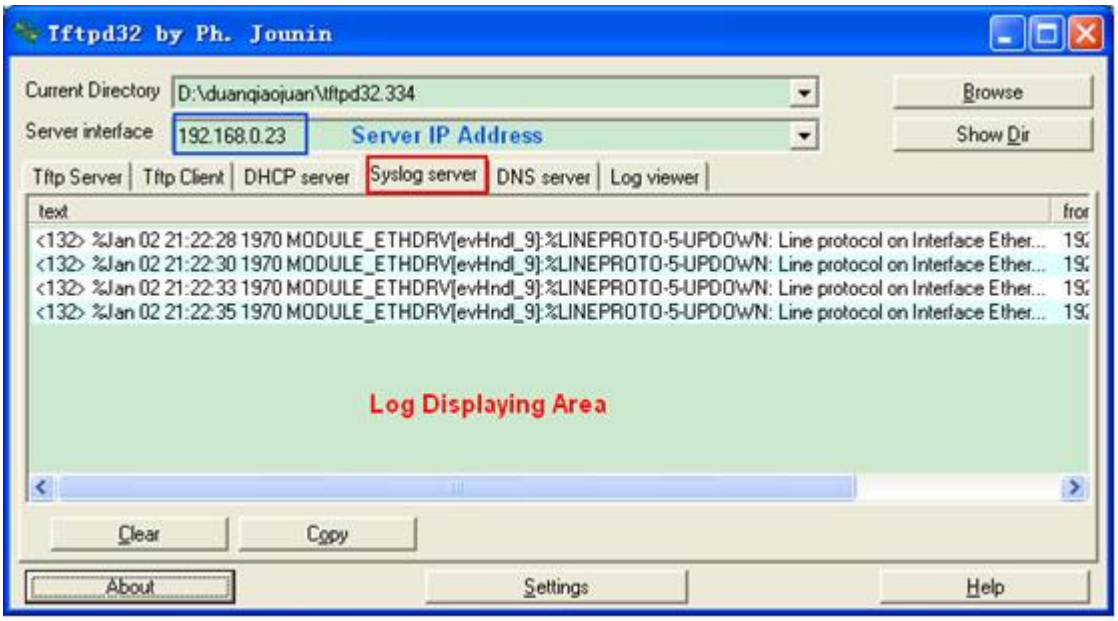


Рис. 255. Загрузка информации системного журнала на сервер в реальном времени

22. Зеркалирование портов (Port Mirroring)

22.1. Введение

Благодаря функции зеркалирования портов, порт копирует все переданные и принятые данные одного порта (порт источника) на другой (порт назначения). Порт назначения, на который передаются данные, как правило, подключается к анализатору протоколов или RMON-монитору, для управления, мониторинга и диагностики неисправностей.

22.2. Описание

Коммутатор поддерживает только один порт зеркалирования, на который отправляются данные (порт назначения), но при этом нет ограничений на количество портов источника. Порты, данные которых зеркалируются, могут быть как в одном VLAN так и в разных. При этом порты источника и назначения зеркалирования также могут быть в одном или в разных VLAN. Порты источника и назначения должны быть разными портами.

Изучение динамических MAC-адресов должно быть отключено на порту назначения.

22.3. Настройка через WEB-интерфейс

1. Настройка функции зеркалирования портов

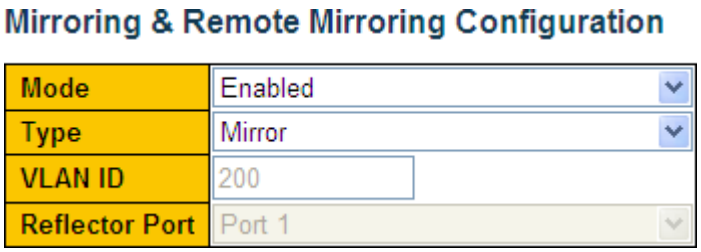


Рис. 256. Настройка функции зеркалирования портов

Режим (Mode)
Опции: Enabled/Disabled (Включено/Выключено).
Значение по умолчанию: Disabled (Выключено).
Функция: включение и отключение функции зеркалирования портов.
Тип (Type)
Опции: Mirror
Функция: настройка функции зеркалирования портов.

2. Выбор порта источника и порта назначения для зеркалирования

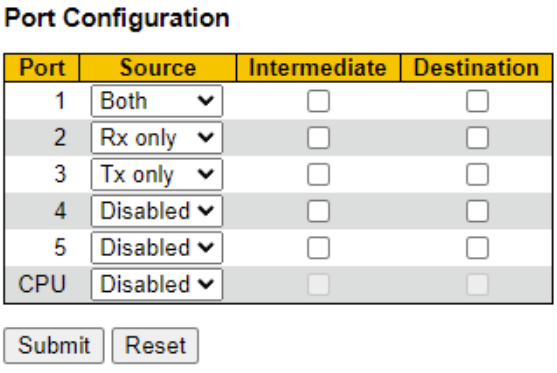


Рис. 257. Выбор порта источника и порта назначения

Порт источник (Source)
Опции: Rx only/Tx only/Both.
Функция: выбор данных для зеркалирования порта источника зеркалирования. «Rx only» означает, что на порту источника отображаются зеркально только полученные пакеты. «Tx only» означает, что на порту источника отображаются зеркально только переданные

пакеты. «Both» означает, на порту источника отображаются зеркально как полученные, так и переданные пакеты.

Порт назначения (Destination)

Функция: выбор порта, который будет портом назначения зеркалирования. Существует один и только один порт назначения зеркалирования.

22.4. Пример типовой настройки

Как показано на рисунке 258, порт 2 - это порт назначения режима зеркалирования, а порт 1 – порт источник. Все пакеты на порту 1 зеркалируются на порт 2.

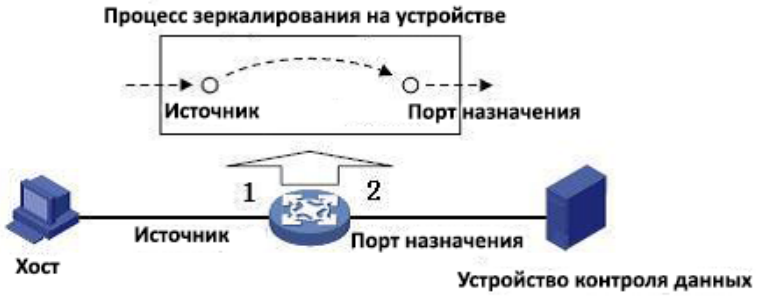


Рис. 258. Пример зеркалирования портов

Процесс настройки:

1. Включите функцию зеркалирования (см. рис. 256).
2. Настройте порт 2 как порт назначения зеркалирования, порт 1 как порт источника зеркалирования, а режим зеркального отображения установите в режим «Both» (см. рис. 257).

23. Диагностика

23.1. Команда Ping

Пользователи могут запустить команду ping, чтобы проверить, доступно ли устройство с указанным адресом и не повреждено ли сетевое соединение во время планового обслуживания системы.

1. Настройка команды Ping

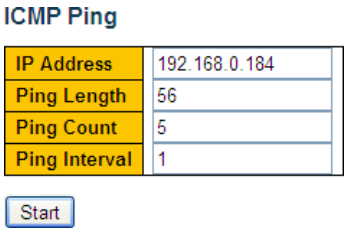


Рис. 259. Настройка команды Ping

IP-адрес (IP Address)
Формат: A.B.C.D.
Описание: настройка IP-адреса удаленного устройства.
IP-адрес (IP Address)
Настраиваемый диапазон: 2 ~ 1452 байт.
Значение по умолчанию: 56 байт.
Описание: настройка длины ICMP-запроса (без учета заголовков пакетов IP и ICMP).
Счетчик Ping (Ping Count)
Настраиваемый диапазон: 1 ~ 60.
Значение по умолчанию: 5.
Описание: настройка количества отправляемых запросов ICMP.
Интервал Ping (Ping Interval)
Настраиваемый диапазон: 0 ~ 30 сек.
Значение по умолчанию: 1 сек.
Описание: настройка интервала отправки запросов ICMP.

2. Просмотр результатов выполнения команды Ping

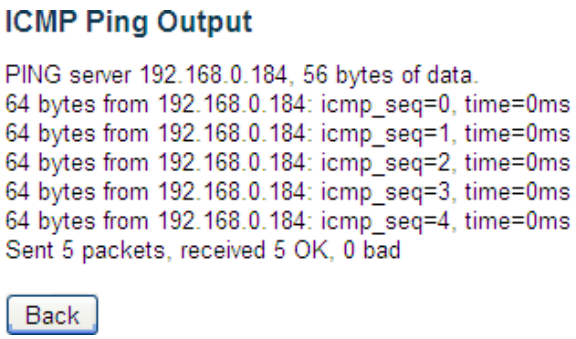


Рис. 260. Отображение результатов выполнения команды Ping

Выходные данные команды ping включают в себя ответ устройства назначения на каждый пакет запроса ICMP и статистику пакетов, собранную во время выполнения команды ping.

24. Расшифровка аббревиатур

Аббревиатура	Полное наименование	Наименование на русском языке
ACE	Access Control Entries	Записи списка контроля доступа
ACL	Access Control List	Список контроля доступа
ARP	Address Resolution Protocol	Протокол определения адреса
BootP	Bootstrap Protocol	Протокол, используемый для автоматического получения клиентом IP-адреса
BPDU	Bridge Protocol Data Unit	Протокол управления сетевыми мостами
CIST	Common and Internal Spanning Tree	Общее и внутреннее связующее дерево
CLI	Command Line Interface	Интерфейс командной строки
CoS	Class of Service	Класс сервиса
CST	Common Spanning Tree	Общее связующее дерево
DHCP	Dynamic Host Configuration Protocol	Протокол динамической настройки узла
DHP	Dual Homing Protocol	Протокол Dual Homing
DNS	Domain Name System	Система доменных имен
DSCP	Differentiated Services Code Point	Точка кода дифференцированных услуг
EAPOL	Extensible Authentication Protocol over LAN	Протокол инкапсуляции пакетов EAP через LAN
GARP	Generic Attribute Registration Protocol	Протокол регистрации основных атрибутов
GMRP	GARP Multicast Registration Protocol	Протокол GARP для регистрации многоадресных групп
GVRP	GARP VLAN Registration Protocol	Протокол GARP для регистрации VLAN
HTTP	Hyper Text Transfer Protocol	Протокол передачи гипертекста
ICMP	Internet Control Message Protocol	Протокол межсетевых управляющих сообщений
IGMP	Internet Group Management Protocol	Протокол управления группами Интернета (протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP)
IGMP Snooping	Internet Group Management Protocol Snooping	Протокол отслеживания сетевого трафика IGMP
IST	Internal Spanning Tree	Внутреннее связующее дерево

LACP	Link Aggregation Control Protocol	Протокол управления агрегацией каналов
LACPDU	Link Aggregation Control Protocol Data Unit	Блок данных протокола управления агрегацией каналов
LLDP	Link Layer Discovery Protocol	Протокол обнаружения уровня канала
LLDPDU	Link Layer Discovery Protocol Data Unit	Блок данных протокола обнаружения уровня канала
MIB	Management Information Base	База управляющей информации
MSTI	Multiple Spanning Tree Instance	Инстанс множественного связующего дерева
MSTP	Multiple Spanning Tree Protocol	Протокол множественного связующего дерева (В один инстанс MSTP могут входить несколько виртуальных сетей при условии, что их топология одинакова)
NAS	Network Access Server	Сервер сетевого доступа
NMS	Network Management Station	Станция управления сетью
NTP	Network Time Protocol	Протокол синхронизации времени
OID	Object Identifier	Идентификатор объекта
PCP	Priority Code Point	Точка кода приоритета
POE	Power Over Ethernet	Технология передачи удаленному устройству электрической энергии
PSE	Power Sourcing Equipment	Источник электрической энергии
PVLAN	Private VLAN	Обособленный VLAN
QCL	QoS Control List	Контрольный лист протокола QoS
QoS	Quality of Service	Качество обслуживания (технология предоставления различным классам трафика различных приоритетов в обслуживании)
RADIUS	Remote Authentication Dial-In User Service	Протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурса
RMON	Remote Network Monitoring	Дистанционный мониторинг сети (расширение SNMP, разработанное IETF)
RSTP	Rapid Spanning Tree Protocol	Быстрый протокол связующего дерева (версия протокола STP с ускоренной реконфигурацией дерева)

SFTP	Secure File Transfer Protocol	Протокол безопасной передачи данных
SNMP	Simple Network Management Protocol	Простой протокол сетевого управления (интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP)
SNTP	Simple Network Time Protocol	Простой протокол синхронизации времени (является упрощённой реализацией протокола NTP)
SP	Strict Priority	Строгий приоритет
SSH	Secure Shell	«Безопасная оболочка», сетевой протокол прикладного уровня
SSL	Secure Sockets Layer	Уровень защищённых сокетов, криптографический протокол
SSM	Source Specific Multicast	Многоадресная рассылка для конкретного источника
STP	Spanning Tree Protocol	Протокол связующего дерева
TACACS+	Terminal Access Controller Access Control System	Система контроля доступа контроллера к терминалам
TCP	Transmission Control Protocol	Протокол управления передачей
UDP	User Datagram Protocol	Протокол пользовательских датаграмм
USM	User-Based Security Model	Модель безопасности на основе пользователей
VLAN	Virtual Local Area Network	Виртуальная локальная сеть
WINS	Windows Internet Naming Service	Служба регистрации и разрешения имен компьютеров
WRR	Weighted Round Robin	Взвешенная очередь